A PROBABILISTIC TECHNIQUE FOR THE ASSESSMENT OF COMPLEX DYNAMIC SYSTEM RESILIENCE

A Thesis
Presented to
The Academic Faculty

by

Michael Gregory Balchanos

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy in the
School of Aerospace Engineering

Georgia Institute of Technology
May 2012

A PROBABILISTIC TECHNIQUE FOR THE ASSESSMENT OF COMPLEX DYNAMIC SYSTEM RESILIENCE

Approved by:

Professor Dimitri Mavris, Advisor
School of Aerospace Engineering
Georgia Institute of Technology

Dr. Neil Weston
School of Aerospace Engineering
Georgia Institute of Technology

Professor Vitali Volovoi
School of Aerospace Engineering
Georgia Institute of Technology

Mr. Frank Ferrese
Naval Sea Systems Command
NAVSEA

Professor Brian German
School of Aerospace Engineering
Georgia Institute of Technology

Date Approved: 11 April 2012

To my Mother Agapi, and my Father Gregory

ACKNOWLEDGEMENTS

The time and effort devoted to the Ph.D dissertation process, is a unique personal journey, that the candidate must take. The outcome of this journey, is the combination of the candidate's own hard work and the guidance or support of several key people that have contributed in their own way over the years to that journey. It is my obligation and pleasure to announce and thank the key people that have contributed on my behalf, for my journey and for the most rewarding experience of my scientific career. However, for every journey, there is always the motivation and the starting point. Going back to my undergraduate student days at the Aristotle University of Thessaloniki, I am thanking Professors George Vougiatzis and the late Symeon Ichtiaroglou for their guidance on completing my senior Degree Thesis. I am also expressing my gratitude to Dr. Elias Aifantis, who helped me build upon my skills that I developed as a physics student, encouraged me to enter the world of engineering, thus allowing me to make the step from physics to aerospace engineering, which was made possible through my admission to Georgia Tech. For the latter, I must thank Dr. Suresh Menon and Dr. Jechiel Jagoda, for giving me the opportunity to make this dream come true.

This dissertation would not have been made possible without the continuous support of my advisor and my committee members. I am very thankful to Dr. Neil Weston, for the time he put into my work, and for all the technical advice and feedback that he provided to me, to ensure the delivery of an uncompromised piece of scientific work. Professor Volovoi's great experience in safety management and reliability engineering has been a great asset to have in this dissertation process. Professor German has offered great support, while his comments were surprisingly insightful,

given that he had less exposure to the topic's evolution to its final form, compared to other committee members. Also, my greatest thanks to Mr. Frank Ferrese, my external committee member, for his real world, technical perspective on my dissertation problem, and for conveying the support of the Office of Naval Research (ONR). He has also been the key link to Icosystem Corporation and Elena Popovici, who not only responded kindly with providing me with a simulation facility for my experiments, but has also offered a lot of her time on for consulting and technical support for my dissertation tasks, thus I would like to thank her very much for her devotion. Last, a big thanks to our ONR program manager, Mr. Anthony Seman, to whom I am very grateful, given that this dissertation would have not become possible, without his insights on improving my work, and without ONR's support.

From the bottom of my heart, I am extending my very special thanks to my academic and research advisor, my committee chair, my mentor, my compatriot, and the best Teacher I ever had, Professor Dimitri Mavris. Dr. Mavris has provided endless and uncompromised support, not by just being my advisor, my boss and a good friend, but also by being a visionary, a fatherly figure that you rely upon in difficult times, and a coach that knows how you must improve yourself, and properly steers you towards achieving this goal. I feel extremely blessed that my Ph.D experience was well beyond the school requirements, it has been a true pedagogical exercise to its fullest. I want to THANK YOU for everything that you have done for me, for allowing me to become a better scientist, a capable engineer, an effective communicator, negotiator, instructor, an inspired and inspiring thinker, a responsible peer, a team player, a good story teller, a stronger personality, but above all, thank you for making me a better person overall. And last, as a fellow Greek, I do stand proud of the fact that our common Greek heritage in philosophy, science, education, and attitude towards life, has been a key inspiration for setting our code of conduct and our way of thinking.

ASDL has truly been my home from an academic, research or employment perspective, while my tenure with the IRIS research team gave allowed me to collaborate with a number of bright and hard working individuals. I would like to mention and thank Matt Konopa, and Santiago Balestrini from the early IRIS days. Payman Touliat, David Fullmer, and Bassem Nairouz have been excellent peers in research, while I am also graced to have them as my closest friends. A special mention goes to Kyungjin Moon, for being a valuable co-author and for voluntarily helping me on carrying out particular thesis tasks. Many thanks to my first ASDL supervisor, Dr. Neil Weston for being a great research mentor, teacher, Ph.D thesis committee member, and friend, as well as Dr. Yongchang Li, for his commitment and continuous support on IRIS research, and on completing my dissertation. Besides IRIS, there have been many other ASDL peers that contributed their own little piece for this dissertation to become a reality. Special thanks to Kelly Griendling and Daniel Cooksey for their friendship and for being there through the challenges and the joys. Same goes to Derya Aksaray, Olivia Pinon, John Salmon, Curtis Iwata and Joe Iacobucci for their friendship, and for sharing their technical skills and experiences. For their willingness to devote time and effort on offering technical and scientific support, I would like to thank Maryon Dong, Ralph Latham, Holger Pfaender, and Yanal Isaac. Last I am expressing my gratitude to Loretta Carroll, Marisol Vega-Holthaus and Megan Halsey, for their outstanding administrative support they have been providing me, both as a student and employee. An additional thank you goes to Dr. Jagoda, for his administrative support, even until the very final moment before this dissertation finds its way on the institution's repository.

Besides my dissertation obligations, I was fortunate to have enjoyed an exciting social life with some good friends I have met here in Atlanta. Starting from the Georgia Tech community, I feel blessed for my friendship with George Stefopoulos, Yorgos Mourlas, Vangelis Farantatos, Vasilis Lakafosis, Yannis Doudalis, and Yannis

Raptis. I was also fortunate to have a larger circle of friends from the Atlanta Greek community: Georgia, Ada, Sophia, Steve, and Raphael, thank you all for being there for me, in all of the good and bad times. I have been lucky to have Professor Christos Alexopoulos, and his wife Aleka, as my close friends and often as my effective family. I would also like to thank Professor Manos Tentzeris, and Professor Wassim Haddad, and his wife Lydia, for their long lasting friendship, for all fun times, and for sharing their good thoughts and ideas with me. I am lucky to also have Atlanta Greek Consul Vasilis Goulousis for his friendship, and for his transfer of wisdom from his own Ph.D experience. Last, I feel blessed that I met and I had Dr. Sissy Petropoulou, who assumed the role of a friend, mentor, my ethical and emotional backup, not giving up on me, even during the times that i would give up on myself. Last, I could not forget my friends in Greece, that despite the eight years that I am away, we managed to keep our frienship fresh as in the early days. Thank you Angeliki Panagiotakopoulou, Nikos Papadopoulos and Angeliki Meliopoulou, Giorgos Pallas, Vasilis Rendoumis and Maria Karampataki. Special thanks goes to my best friend, Dimitris Katsoulis, who has been the person that introduced the idea of applying to Georgia Tech, and I am very happy that he did.

Concluding this section, I am extending my greatest thanks to my family, both in the US and in Greece. Many thanks to my aunt Chrys, my uncle Constantine, and my cousins John, and Dimitri, for their love, support and for motivating me to continue my graduate studies in the USA, as well as for their hard work on making it happen. Last, but by no means with the least importance, I would like to thank my parents, Agapi and Gregory Balchanos. They have always been there for me for my entire life, for all decisions I have made, no matter how hard they could have been for them. I love you both as nothing else in this world, and thus I am devoting this dissertation to you, just to say a big thank you for who I am and what I have become with your endless love and support.

Thank you all!

Michael Balchanos

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

SUMMARY

In the presence of operational uncertainty, one of the greatest challenges in systems engineering is to ensure system effectiveness, mission capability and survivability for large scale, complex system architectures. Historic events such as the 2003 Northeastern Blackout, and the 2005 Hurricane Katrina, have underlined the great importance of system safety, and survivability. With safety management currently applied on a reactive basis to emerging incidents and risk challenges, there is a paradigm shift from passive, reactive and diagnosis-based approaches to the development of architectures that will autonomously manage safety and survivability through active, proactive and prognosis-based engineering solutions. The shift aims to bring safety considerations early in the engineering design process, in order to reduce retrofitting and additional safety certification costs, increase flexibility in risk management, and essentially make safety be "built-in" the design.

As a possible enabling research direction, resilience engineering is an emerging discipline, pertinent to safety management, which offers alternative insights on the design of more safe and survivable system architectures. Conceptually, resilience engineering brings new perspectives on the understanding of system safety, accidents, failures, performance degradations and risk. A resilient system can "absorb" the impact of change due to unexpected disturbances, while it "adapts" to change, in order to maintain the system's physical integrity and capability to carry on with its mission. The leading hypothesis advocates that if a complex dynamic system is more resilient, then it would be more survivable, thus more effective, despite the unexpected disturbances that could affect its normal operating conditions.

For investigating the impact of more resilient systems on survivability and safety, a framework for theoretical resilience estimations has been formulated. It constitutes the basis for quantitative techniques for total system resilience evaluation, based on scenario-based, dynamic system simulations. Physics-based Modeling and Simulation (M&S) is applied for dynamical system behavior analysis, which includes system performance, health monitoring, damage propagation and overall mission capability.

For the development of the assessment framework and testing of a resilience assessment technique, a small-scale canonical problem has been formulated, involving a computational model of a degradable and reconfigurable spring-mass-damper SDOF system, in a multiple main and redundant spring configuration. A rule-based feedback controller is responsible for system performance recovery, through the application of different reconfiguration strategies and strategic activation of the necessary main or redundant springs. Uncertainty effects on system operation are introduced through disturbance factors, such as external forces with varying magnitude, input frequency, event duration and occurrence time. Such factors are the basis for scenario formulation, in support of a Monte Carlo simulation analysis. Case studies with varying levels of damping and different reconfiguration strategies, involve the investigation of operational uncertainty effects on system performance, mission capability, and system survivability. These studies furthermore explore uncertainty effects on resilience functions that describe the system's capacities on "restoring" mission capability, on "absorbing" the effects of changing conditions, and on "adapting" to the occurring change.

The proposed resilience assessment technique or the Topological Investigation for Resilient and Effective Systems, through Increased Architecture Survivability (TIRESIAS) is then applied and demonstrated for a naval system application, in the form of a reduced scale, reconfigurable cooling network of a naval combatant. Uncertainty effects are modeled through combinations of different number of network fluid leaks.

The TIRESIAS approach on the system baseline (32-control valve configuration) has allowed for the investigation of leak effects on survival times, mission capability degradations, as well as the resilience function capacities. As part of the technique demonstration, case studies were conducted for different architecture configurations, which have been generated for different total number of control valves and valve locations on the topology.

CHAPTER I

INTRODUCTION

1.1 The need for effective military systems

Throughout most of the history of humanity, warfare has been the traditional means for a nation to ensure national security and internal social stability [222]. However, the model of warfare has evolved from raw military force projection to a multidimensional approach, with science, technology, tactics, and intelligence playing an important strategic role [157]. In this paradigm shift, science and technology [208] have been the essential drivers for military system development and acquisition, also leading to significant advances in military capability.

Advancement in overall system capability has been raising concerns over safety and security, both at regional and national scales. If utilized and operated by the inappropriate entities, in different applications, the same technologies can become severe threats against the nation's security. For instance, nuclear reactors are built as industrial power plants for energy generation and distribution. At the same time however, nuclear technology is the basis of weapons of mass destruction (WMD), nuclear or chemical [23], that could enable acts of terrorism. The possibility of improper implementation and use of technology, in accordance to national security concerns, brings attention in investments for better safety and survivability.

The risk of emerging threats, when system capability and advanced technology are utilized with malicious intent is not the sole driver for increased safety and survivability. Increased capability itself results in larger scale complex systems [11] with more interconnections and modes of operation. A natural consequence is that a complex system has more opportunities to experience faults, either natural or intentional,

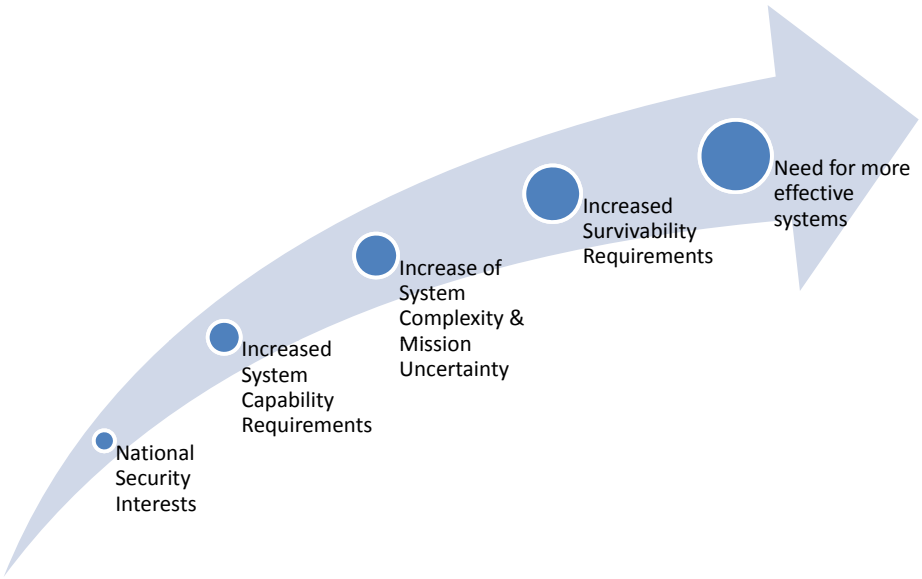


Figure 1: Motivation thought path towards the need for effective systems

that could result in higher risk of local failures, or eventually to total system collapse [51]. Thus, capability results in more complex systems with possibly higher susceptibilities/vulnerabilities, that eventually contribute to an increased uncertainty in mission performance and degrade system survivability and safety. This thought path drives the motivation for this research, as illustrated in Figure 1, and is the basis of establishing a general need for more effective military systems.

1.1.1 National security interests

In a globalized framework of socio-economical growth, nations have shifted towards new means of pursuing political and economic affluence. For ensuring national security and local/global socio-economical stability, practice of diplomacy and political alliance through collaboration [116] have become the main substitute of traditional forms of warfare-based resolution of conflict. In support of the previous statement, it has been observed that, since the end of World War II, humanity has been experiencing a time period with the most peace agreements, compared to any other period in world human history, and as Wallensteen [255] indicates, there have been more

conflicts than ever, which have either been prevented or entirely avoided.

The role of National Security is crucial for allowing nations to mitigate conflict and contribute towards global peacekeeping. For the U.S. Government, the Nation's security is a top priority [60]. The original national security initiative has been introduced by President Truman through the National Act of 1947, and is defined as "the foundation for the development of valid national objectives that define U.S. goals or purposes" [59]. In particular, National Security interests include preserving the U.S. political identity, framework, and institutions, fostering economic well-being, and bolstering international order supporting the vital interests of the United States and its allies [242].

Observation 1.1: National Security interests are crucial for political, social and economical stability, either at national or international levels.

1.1.2 Increased system capability requirements

As part of the U.S. National Security Strategy, the Department of Homeland Security (DHS) is responsible for monitoring the application of technologies for good civilian purposes. Most DHS mandates require more capable systems in support of security, in the form of military and defense systems, infrastructures or other advanced technological equipment [201]. The U.S. Department of Defense (DoD) is also advocating for more capable systems [123], through development of their DoDAF standard [55]. DoDAF is a standard framework for defense systems acquisition, with capability as the main driving objective, leading the way for *capability-based design and acquisition* [24], as an emerging branch of systems engineering.

The U.S. Armed Forces have based their military goals on system capability, as it is expressed through their doctrine [240]. Military doctrine describes how to best make use of military power in support of military operations, and strategy in order to accomplish national political objectives [202]. It is a form of "constitution" that

guides actions toward well-defined goals and provides the basis for mutual understanding within and among the services and the national policymakers [163].

The US Air Force maintains a three tier (basic, operational, tactical) capability-driven doctrine [237] that requires advanced, highly effective, lethal and non lethal systems with unique capabilities [213] across the range of military operations [202]. The U.S. Navy doctrine is aligned to the objective of attaining national policy objectives through capacity to wage war successfully [163]. With the recognition of diversity and multi-dimensionality of modern warfare, the importance of readiness, flexibility, sustainability, and mobility in military operations is underlined, thus suggesting requirements for multi-terrain capability, in support of survival and combat effectiveness [247] of Navy forces [163]. The U.S. Marine Corps doctrine brings focus on the force of human to resolve and utilize technology to leverage the chaos and complexity of the battlefield [244]. For adapting available resources in chaotic and austere operating environments, capability is a key enabler [243]. The U.S. Coast Guard is protecting the nation's borders and territories, through missions that require the right assets and capabilities at the right place and time [239], while expecting demonstration of fighting flexibility, properly managing risk and being restraint based on long term mission goals. Last, the US Army's primary focus is land warfighting, underscoring the need for capability and credibility in full spectrum operations [238]. Concluding, the literature search has collectively revealed that doctrine implies that military systems must be designed and tested for being able to provide advanced capabilities, multi-domain superiority and improved system and mission effectiveness.

Observation 1.2: National Security interests drive the need for increased capability, as resulting from strategic and doctrine-based reasoning.

1.1.3 Increase of system complexity & mission uncertainty

There are several options on how systems are designed for increased capability. Common approaches include the addition of redundant subsystems [16] or technology infusion [24]. In all cases, the expected benefits concentrate on increased functionality and extended frames of operation. For the former approach, the system boundaries are extended, with an increased number of subsystems and interconnections, which result in increasing the overall system complexity [38]. While there has been some diversity on how system complexity is understood, defined [88] and measured [7], [51], [49], it is commonly accepted that increased system complexity increases uncertainty in mission performance. Thus, complexity is responsible for higher risks of faults that may lead to larger scale failures, total system shutdowns [122], performance degradations or other forms of emerging behavior [20]. Technology infusion may also be responsible of different forms of complexity, that could be additionally attributed to technology readiness levels (TRL) or other factors associated to the particular technology implementation.

In all cases, the higher uncertainty in normal system operation and mission effectiveness due to system complexity, results in risks on the levels of system safety and survivability. From a safety standpoint, complexity effectively introduces additional modes of failure, or brings more opportunities for performance degradation. If safety, reliability and availability requirements are not met throughout a system's mission, then overall system survivability is reduced, thus significantly impacting total system effectiveness. In an alternative formulation of the earlier assertion, a complex structure is more fragile, or equivalently less *resilient*, as fragility is complementary to resilience [146].

Observation 1.3: Increased system capability is often achievable at the cost of increasing system complexity, operational uncertainty and risk.

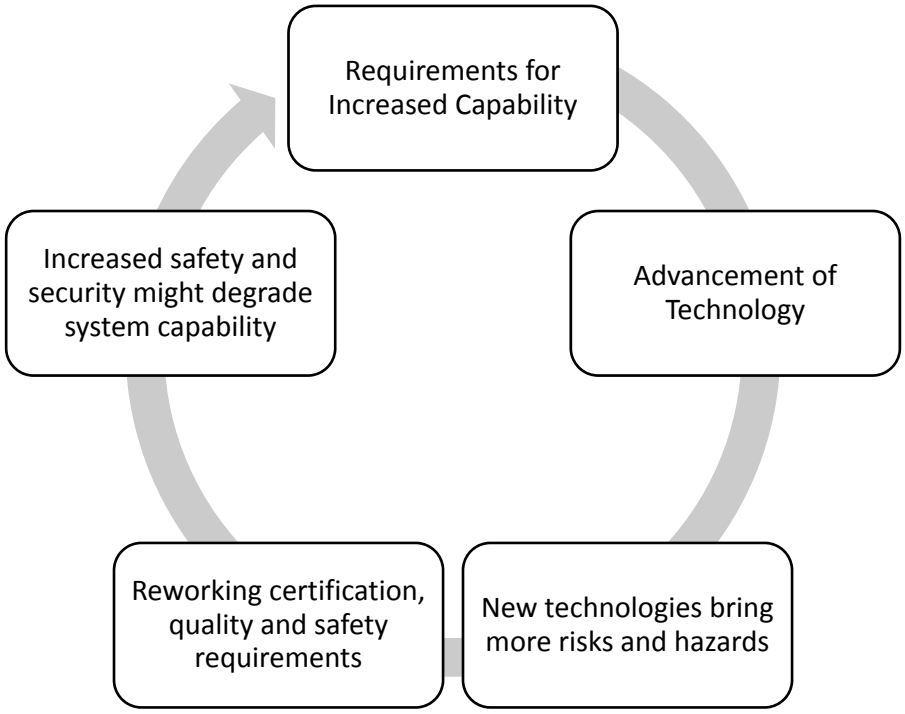


Figure 2: Advanced capability requirements lead to increased safety requirements

1.1.4 Increased survivability requirements

Advancement of technology has lead to more capable systems with multiple mission abilities. The enhanced functionality extends the envelope of system operation, thus introducing forms of uncontrolled uncertainty, either related to human-system interactions or incompatibility with existing SoA systems. Other emerging challenges, such as technology immaturity, or how these are integrated to existing system architectures, introduce additional layers of uncertainty, thus contributing to increased risks or additional safety hazards. Consequently, increased technological ability has brought exposure to additional hazards and increased risk levels.

To compensate for increasing risk in complex system operations, the responsible government parties have been continuously reworking certification and quality requirements for hazard and risk mitigation in military or commercial system acquisition. Operations and system design requirements are constantly revised to address

the additional risks and hazards, in order to ensure that system and human safety are maintained. In many cases, advanced technologies are necessary to satisfy more demanding certification requirements, which target system safety, security, survivability, and overall risk mitigation [217].

At this stage, there is a strong possibility that system capability may be ultimately degraded, as a consequence of performance degradations due to either weight addition, or further complexity increase. Technology infusion that is dedicated to safety management, may itself be at a low *Technology Readiness Level* (TRL) [148], thus leading to further safety requirements. Within the engineering requirements definition phase, there is an overall cyclical process driving both the capability and safety requirements at an alternating iterative fashion, until satisfactory compromise is achieved and is visually explained in Figure 2.

Observation 1.4.1: System capability implies increasing safety, security and survivability requirements, which may need to be iteratively revised and expanded, under the presence of technology uncertainty, if desired capability levels cannot be reached.

From an economic perspective, traditional design approaches for safety can rarely be justified as the most cost-effective [41]. In most cases, improved safety implies increased weight and cost, thus inversely affecting affordability. According to the current State-of-the-Practice (SoP), system architectures are optimized for performance and capability at the conceptual and preliminary design phase, while system certification and other safety concerns are addressed at the latter design phases. As explained earlier, this practice often results in selecting additional technologies for enhancing system safety and reliability, that designers then need to retrofit in the architecture at latter design stages. Late or post-design retrofitting approaches for enhancing safety may not be adequate in the long term [195]. As demonstrated

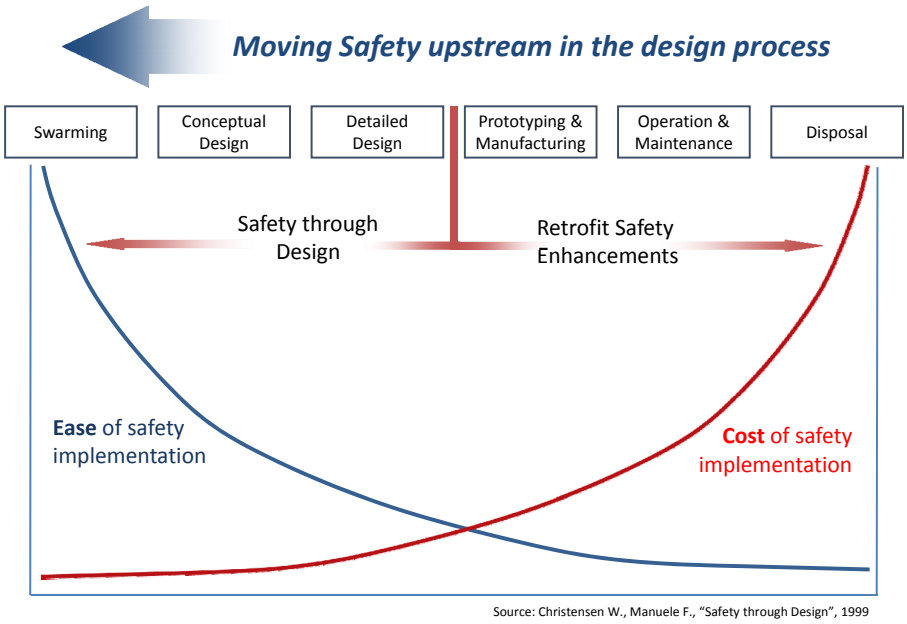


Figure 3: Safety early in the design process [41]

in Figure 3, Christensen has suggested that by incorporating design considerations for safety objectives in the conceptual design phase, architectures will be capable of seamlessly accommodating safety enhancements and equipment, thus avoiding any necessary costs for late-stage retrofitting [206].

The importance of early investment [218] in system safety and survivability for military system acquisition, has been emphasized by several aerospace and naval authorities, agencies and domain experts. The JTCG/AS Survivability Handbook Series states that "survival of our forces is a crucial aspect of full-spectrum dominance of our enemy - an aspect that increases in complexity as the battlefield arena becomes more complex" [209]. The DoD through their DOD Regulation 5000.2-R indicates that "mission-critical systems, including crew, shall be survivable to the threat levels anticipated in their operating environment" [58].

Observation 1.4.2: Investing on safety management at early stages of the system design and acquisition process, implies benefits program affordability, seamless integration of subsystems and technologies, as well as fewer iterations until compromise

of capability, safety and survivability is achieved, while minimizing risk due to technology infusion and operational uncertainty.

1.1.5 Closing the loop: Need for more effective systems

Given the importance of system capability and safety management in military system design and acquisition, an opportunity is becoming apparent for the research investigation towards more effective systems. In its short definition, system effectiveness is a measure of the ability of the system to accomplish its objective [97]. However, under a quantitative format, system effectiveness is a cumulative representation of a system's capability, survivability and overall safety and availability [97]. Following on the previous statement and observations, Figure 4 summarizes the reasoning process towards the need for more effective systems. This opportunity is of event greater importance, given that there haven't been any globally established standard design methods for designing military systems that can be always fully capable, available and survivable at any time during their mission.

Observation 1.5: Driven by the guidance of National Security interests, the need for more capable, safe/survivable systems under affordable system design and acquisition processes, investigation of the concept of system effectiveness is the leading research objective.

1.2 The vision for more survivable and affordable naval combatants

The U.S. Navy is interested on new design approaches for improving mission effectiveness of their assets during combat operations. As outlined by Habayeb [97], system effectiveness depends on system capability, availability and survivability. The exceptional importance of survivability in contributing to system effectiveness has been

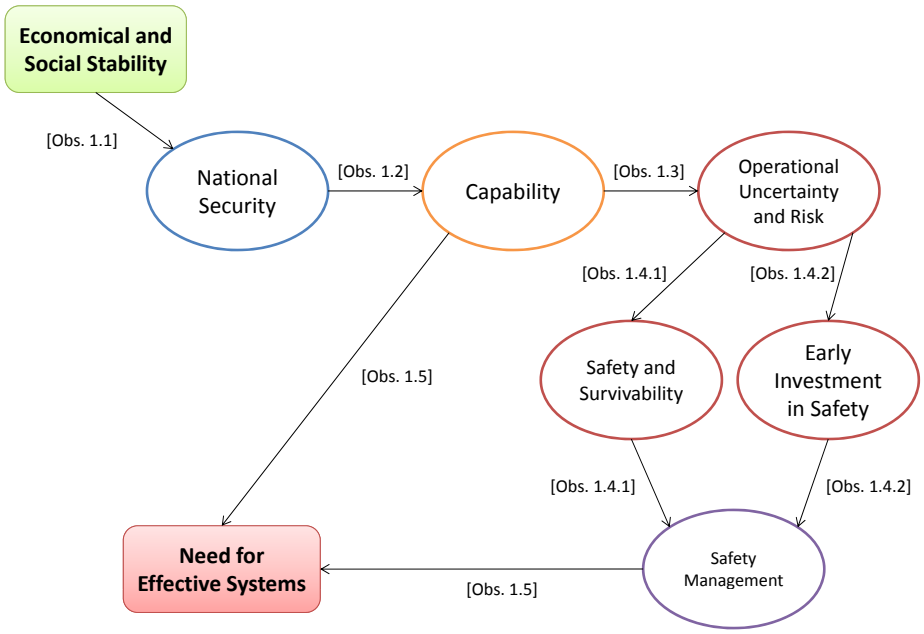


Figure 4: From National security to more effective military systems

recognized by the naval engineering community. As Rains points out, system effectiveness and survivability should be treated as attributes early in the design process [182]:

"Combatant ship design is a series of tradeoffs often made with little knowledge of the impact of the decisions, except on ship size or displacement. However, many other considerations, such as combat effectiveness, survivability, and initial cost may be equally important in the design process".

1.2.1 System survivability

System effectiveness however is by no means exclusively system-centric. It does depend on the various modes of *change* that occur around or within the system. These modes range from the threat environment that the system needs to operate in, the evolution of its mission portfolio, as well as its own natural evolution, regarding

its operational health and military worth and capability. In a threat or accident-free environment, system effectiveness is primarily driven by mission capability and availability. However, under increased threat levels, survivability is what practically determines the overall effectiveness.

Figure 5 presents some historical incidents, involving significant attacks or accidents on naval ships. All ships have been designed with certain performance criteria, as well as advanced capability considerations, which they demonstrated under normal operating conditions. The historic incidents of Figure 5 are representative of the typical challenges during a destroyer's mission. These range from tactical attacks through missile or torpedo, or accidental incidents, such as malfunction or human error. The high uncertainty around incident occurrence and progression, does not allow to easily identify the design solutions that would almost guarantee the same levels or performance and capability, as in under normal conditions. Thus, an opportunity is arisen to investigate how well would the vessel maintain its by-design performance and capability in operating circumstances under high vulnerability and degraded system health.

Observation 1.6.1: In order to design more effective systems, not only the designer must have expected performance and capability levels in mind, but also consider survivability and investigate how the system performs in high threat intensity environments under degraded figures of merit.

1.2.2 System affordability

Change of fiscal nature significantly affects the resources committed for R&D, testing and the overall system acquisition costs. With the expected budget constraints that aim for lower acquisition costs, yet with no discount on required performance and capability, the problem of viability becomes very challenging [152]. Combined to the

1967

USS Forrestal (CVA 59)

- Incident: ZUNI rocket fired accidentally
- Damage: Extensive structural damage, loss of equipment
- Casualties: 161 Injured, 134 Killed
- Cost: $72 Million

1987

USS Stark (FFG 31)

- Incident: Struck by 2 Exocet missiles
- Damage: Extensive structural damage, almost sank
- Casualties: 5 Injured, 37 Killed
- Cost: $142 Million

1988

USS Samuel B. Roberts (FFG 58)

- Incident: Struck an M08 mine
- Damage: DIW, almost sunk
- Casualties: 69 Injured, 0 Killed
- Cost: $32 Million

1989

USS White Plains (AFS 4)

- Incident: Human error, fuel ejection valve
- Damage: DIW
- Casualties: 161 Injured, 6 Killed
- Cost: $33 Million

2000

USS Cole (DDG 67)

- Incident: Terrorist attack
- Damage: DIW
- Casualties: 36 Injured, 17 Killed
- Cost: ~$200 Million

Figure 5: Historical naval attack incidents and accidents

additional requirements on increased survivability for maximizing overall effectiveness, the problem of affordability while maintaining effectiveness becomes another opportunity for investigating revolutionary configurations, technologies or total design methods that could identify a viable compromise on all fronts.

Budget constraints are critical for determining the mission portfolio of a military system, based on operating, maintenance and disposal costs. It could put limitation on system capability and if a good balance between cost and effectiveness cannot be kept, there is risk in returning a solution that is affordable, yet very limited against its expected mission effectiveness. Up to recent, the Navy has discovered the major contributions to increasing development and maintenance costs for its naval fleets. Figure 6 shows the Navy budget breakdown over the years, including navy personnel compensations, ship operations and maintenance, as well as shipbuilding and conversion costs. In Figure 7, a yearly analysis (FY03) of the cost per hull is presented for a DDG-51 naval destroyer. In both studies, the need for crew rightsizing is underlined, as personnel costs (shown in red) represent more than half of the Navy's budget for a given year.

Observation 1.6.2: As system effectiveness is directly linked to operational figures of merit (e.g. performance, capability and survivability), one must consider additional indirect factors, in the form of budget constraints, cost reduction and affordability initiatives. System effectiveness must come without compromise, yet at the lowest possible acquisition and operation costs.

Connecting with earlier thoughts, modern naval ships comprise of many interdependent subsystems, as other large scale engineering systems. Critical issues around large scale systems, is robustness and surviving external disturbances or full scale attacks, while maintaining their expected mission capability levels. All naval ships use

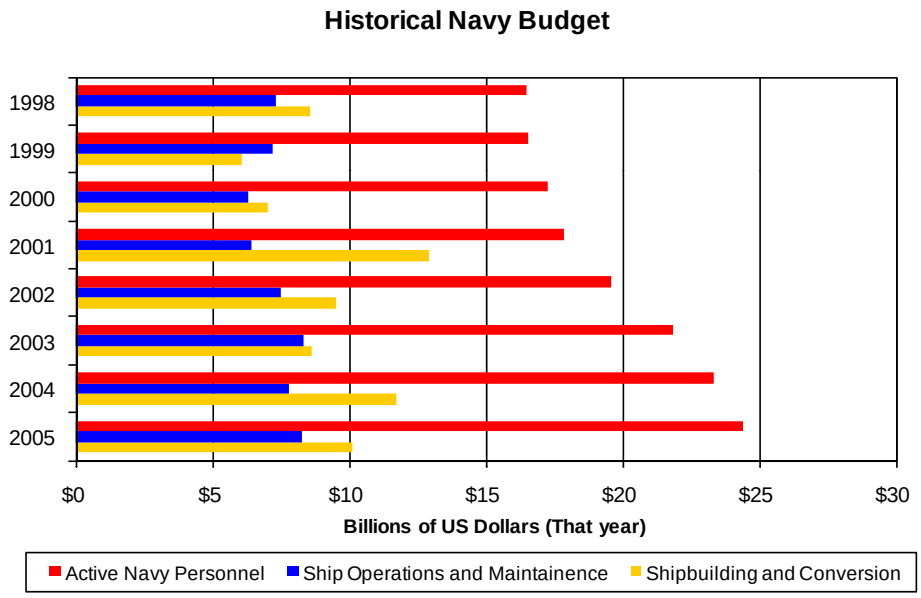


Figure 6: Historical dominance of personnel cost in Navy budget [199]

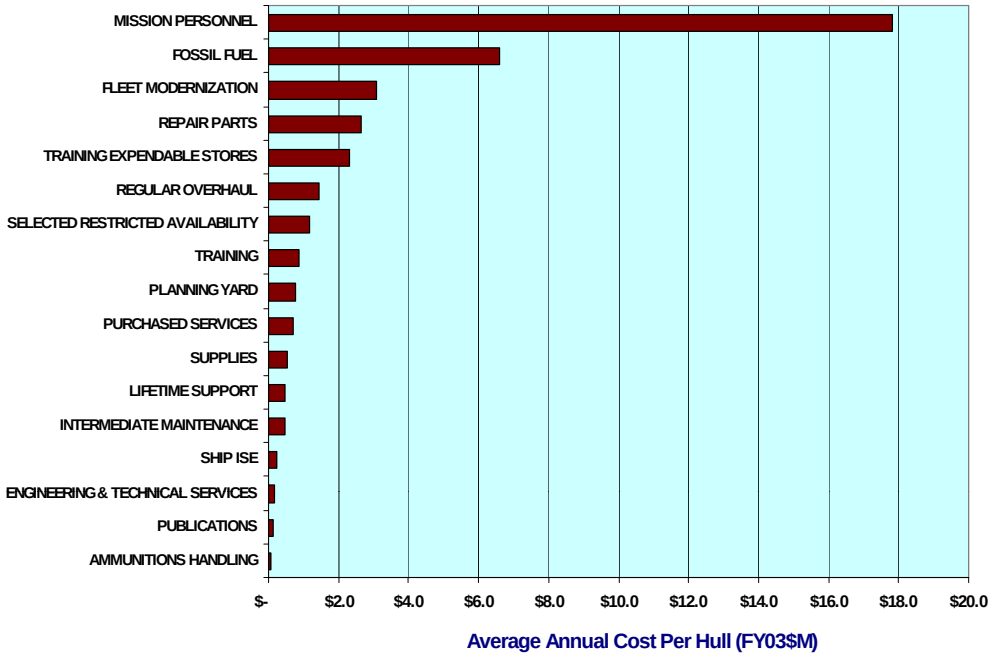


Figure 7: Average annual cost per hull [86]

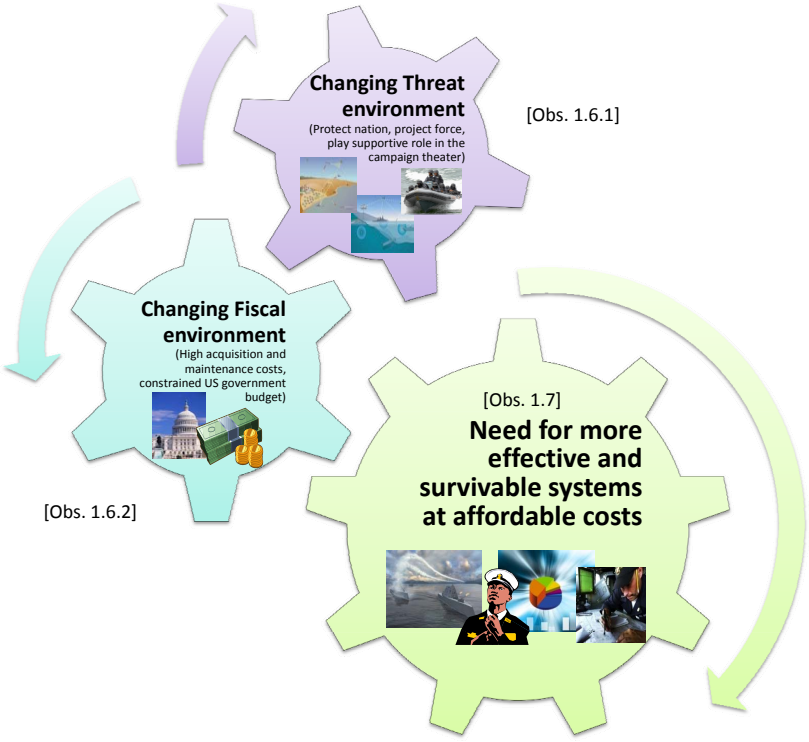


Figure 8: The need for more survivable and affordable naval systems

human-in-the-loop communications and decision making, resulting increased ownership cost.

Doerry has underlined that "for maximum effectiveness at lowest costs, survivability should be an important consideration for the design of the system architecture of each mission and distributed system as well as the physical arrangements of system elements on the ship" [65]. In other words, with survivability design considerations in the early conceptual design phase, enabled by system reconfigurability and automation, the naval combatants of the future are expected to have right-sized crews, thus reducing total ownership costs. In conclusion, as Figure 8 demonstrates, the rapidly changing fiscal and threat environment regarding the development and operation of naval vessels, demands for a shift towards design for system effectiveness, that is mainly driven by system survivability and affordability.

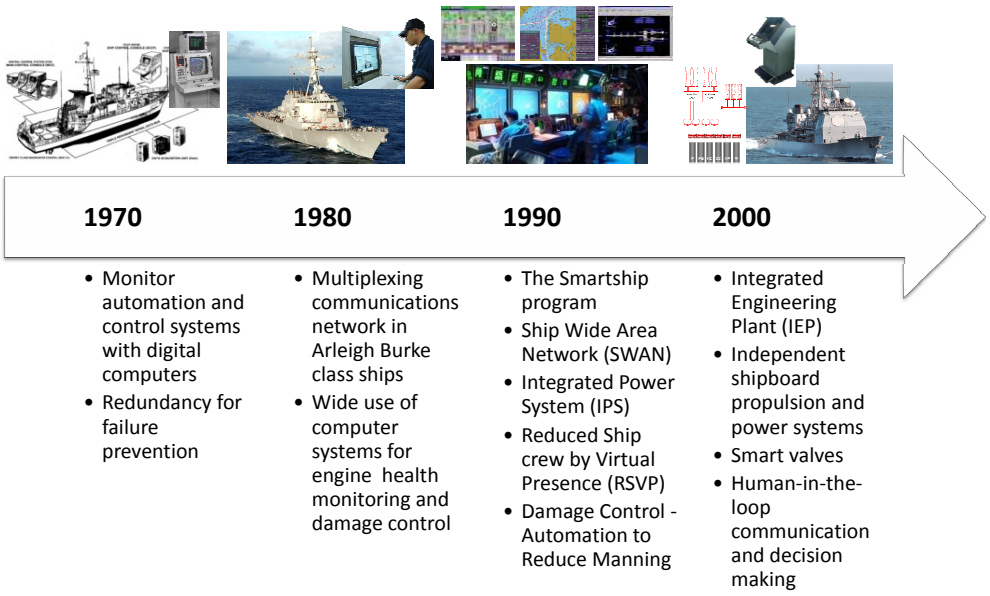


Figure 9: Efforts to improve naval system effectiveness, survivability and automation

Observation 1.7: Naval system design must bring more emphasis on reducing operating costs and manning workload, while increasing survivability, reliability and fight-through capability, for most of the system's lifecycle [5].

1.2.3 Recent efforts towards effective and efficient naval systems

Today's conventional ships have independent shipboard propulsion and electrical power plants with centralized systems associated with the rest of the shipboard engineering plant and machinery infrastructure [144]. Under their vision for increased survivability and affordability, the U.S. Navy is investigating alternative system integration strategies. Several efforts have been initiated, in order to address the Navy's direction towards crew right-sizing, increased levels of automation and operational flexibility, with a time line of these efforts presented in Figure 9.

1.2.3.1 The Integrated Power System (IPS) architecture

A first attempt was recorded under the proposal for transitioning to the Integrated Power System (IPS) architecture [28]. The IPS relies on two main and two auxiliary

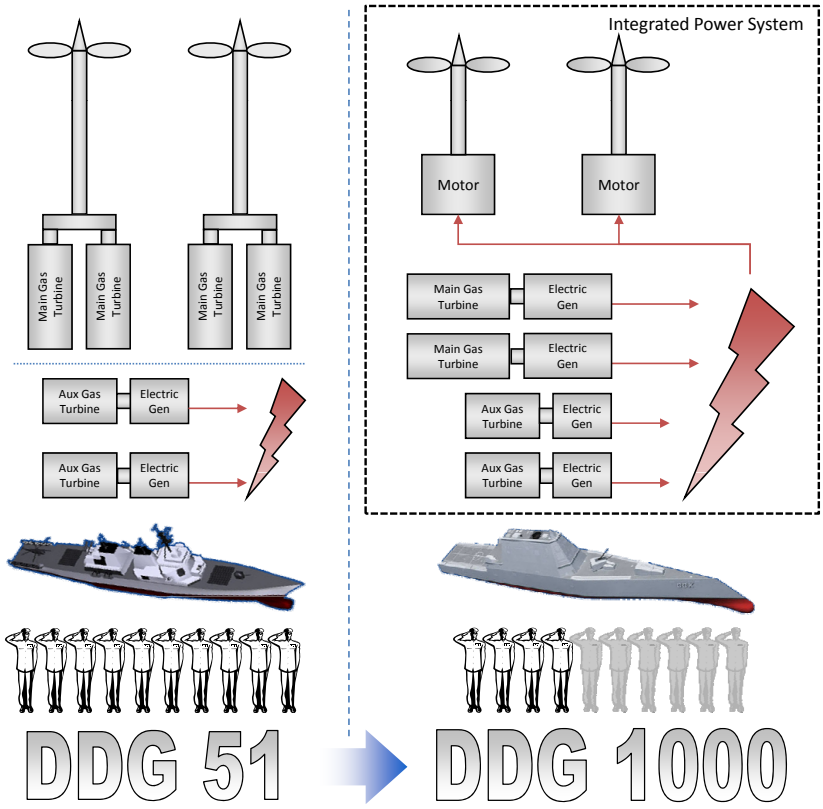


Figure 10: Zumwalt class with right-sized crew and integrated power plants

power plants that generate the total amount of power that the ship needs for performing its basic functions and operations. Power to all loads is dynamically distributed, according to mission expectations, strategic planning and availability of resources [66]. As Figure 10, suggests, IPS-based architectures are expected to bring more flexibility in resource management, along with the reduced crew sizing requirements [44].

1.2.3.2 The SmartShip program

The Smart Ship program was initiated by is the US Navy and Coast Guard and demonstrated what a small amount of automation can produce in terms of added capabilities and reduced costs [224]. The USS Yorktown (CG-48) was modified and automated to reduce the workload, manpower requirements and cost while enhancing the combat readiness and quality of life of the crew [67]. It incorporated damage

control [103] and engineering systems which automated many of the routine daily tasks [135].

1.2.3.3 The Integrated Engineering Plant (IEP)

The next-generation multi-mission destroyer, the DDG-1000 has been envisioned to be operated by a crew of 150, in a more than 50% reduction when compared to DDG-51 and subsequent Arleigh Burke class destroyers [246]. As a possible enabling strategy, the Office of Naval Research (ONR) proposed the Integrated Engineering Plant (IEP) concept in 2001 [70]. The IEP is a vision for a notional ship architecture that is removing traditional system-level barriers [229], between various ship plants, while integrating the ships engineering and resource allocation systems, including the electrical, propulsion and auxiliary systems [268]. The resulting architecture consists of a highly dynamic, decentralized and interdependent set of distribution networks, in which plant components are organized in layers and can perform the predefined or self controlled tasks [144], as explained in Figure 11 [226]. With the modular IEP architecture and optimal maintenance procedures, total ownership costs are expected to be reduced. The IEP builds upon knowledge acquired through the IPS initiative, and has inspired further initiatives, such as the Reduced Ship Crew by Virtual Presence (RSVP)[210] and the Damage Control - Automation to Reduce Manning (DC-ARMS) concepts [263].

Besides flexible architectures [144], resource management [268] and crew right-sizing [68], through the IEP, the U.S. Navy is addressing the fact that naval ships are becoming more complex, as they are comprised by an increasing number of heterogeneous interdependent subsystems. This increased complexity requires new methods for the design and operation of these naval systems [115]. The *Integrated Reconfigurable Intelligent Systems* (IRIS) initiative by the Aerospace Systems Design Laboratory (ASDL) at Georgia Tech [5], has been introduced as a response to the U.S.

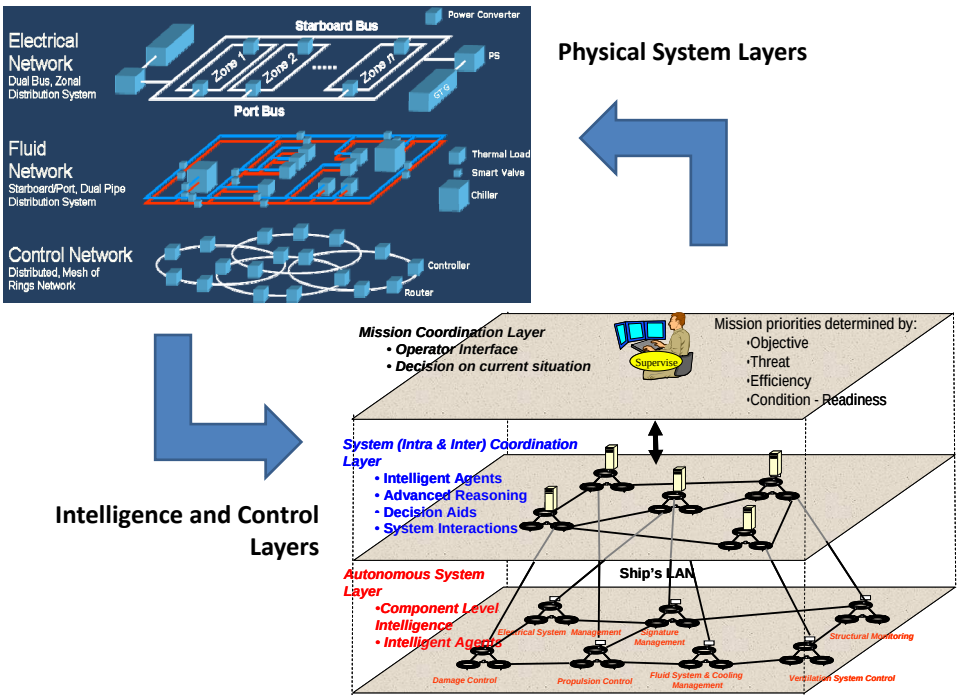


Figure 11: The IEP concept [253]

Navy's IEP vision for the future naval combatant. Following the IEP vision, an IRIS ship should be capable of:

Provide continuous communication, mobility, power, and thermal management for all shipboard systems, even during major disruptions involving cascading failures, thereby reducing manning requirements and increasing overall ship effectiveness. [5]

As a design exercise, under the IRIS initiative, a systems engineering framework [205] is formulated for investigation of naval system design solutions with increased automation and reconfigurability [68], and implemented through distributed, intelligent control architecture [115]. As a result, these intelligent platforms must be capable of autonomously executing a trio of basic functions, as explained in Figure 12. Aligned with the U.S. Navy's outlook, the overarching objective of IRIS is to propose solutions for more survivable, reconfigurable and affordable naval ships, in an effort to reduce total ownership costs and increase mission and system effectiveness.

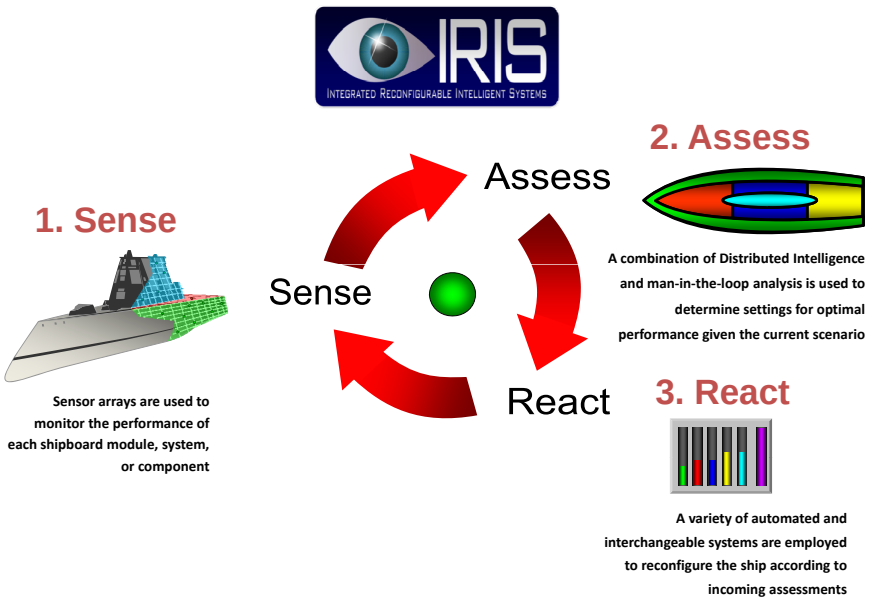


Figure 12: IRIS functionality [115]

1.3 Enabling directions: Safety Management

The vision for more effective systems has initiated the inspiration for this research. But as a requirement at the higher level of abstraction, one may wonder how can this vision be interpreted at a lower, more technical level. It is thus necessary to investigate how system effectiveness is further broken down into contributing concepts, that could potentially become major research thrusts. Based on literature search, an overview of system effectiveness and its components is presented in Appendix A, mainly as suggested through the work of the Military Operations Research Society (MORS).According to this framework, system effectiveness is dependent upon three contributors, system availability, dependability and capability [97]. In a mathematical form, system effectiveness is a probability and is the product of the probabilities for the three contributions, as given by Equation 1.

$$P_{SE} = p_{Availability} \cdot p_{Dependability} \cdot p_{Capability} \tag{1}$$

1.3.1 "Change" as a determining factor of system effectiveness

With the broad nature of the concept of system effectiveness, one would wonder which component should receive most attention, as part of the research objectives. These three "-ilities" are not static design attributes, they are dynamic figures of merit that depend on the change that the system and its environment is experiencing. The world evolves due to a number of changes that occur and that can be the result of other pre-occurring changes. Many distinguished philosophers have attempted to interpret *change*. Heraclitus of Ephesus (535 B.C. - 475 B.C.) was one of the first to mark the significance of change in the real world, summarizing it through this simple, yet so powerful expression:

"$\tau\acute{\alpha}\ \pi\acute{\alpha}\nu\tau\alpha\ \rho\varepsilon\tilde{\imath}$" ("Everything flows")

Change refers to actions that result in altering one or more state properties that describe the condition, in which a system finds itself. Change happens over the lapse of time, implies transition of system location, system composition (e.g. natural aging) or operating status. Change does not always have to cause adversity, thus change is often part of the system's overall evolution, in terms of its physical composition, mission capability and total environmental conditions (physical or fiscal).

In many cases however, change can trigger non-favorable, adversary, single or multiple disturbance events. Depending on the system, the mission and the typical operating conditions, adversary change leads to increasing threat levels that further result in increasing safety risks, survivability reduction, mission capability and system health degradation, with an overall impact in system effectiveness [198].

In larger scale complex systems, describing change is a challenging task. Attributes of change with respect to the mission and health of the system must be defined. For instance, change in terms of origin can be *endogenous* or *exogenous*. The 2005 Hurricane Katrina and the 2003 Northeastern Power Blackout are representative historical

events for exogenous and endogenous change respectively. The 2005 Hurricane Katrina was the sixth strongest overall, as well as one of the five deadliest in the history of the United States [132]. When the levee system catastrophically failed, most of the city of New Orleans had flooded, with at least 1,836 people having lost their lives in the actual hurricane and the subsequent floods [169]. The 2003 Northeastern Power Blackout was initiated by a local power substation failure, resulting in a massive propagation of malfunctions in power generation and delivery, water supply and communications. A generating plant in Eastlake, Ohio went offline amid high electrical demand, followed by the high-voltage power lines later going out of service. More than 508 generating units at 265 power plants during the 4-day outage were shut down, affecting an area with an estimated 50 million people and 61,800 megawatts (MW) of electric load in 8 US States, and the Canadian province of Ontario [84]. At least eleven fatalities were recorded, and brought the total costs in the United States ranging between $4 billion and $10 billion (2003 U.S. dollars) [169].

Another attribute is intent of a threat. Changes can emerge due to *natural* threat, or due to malicious actions, either in the forms of *malevolent* attacks, or asymmetric threats. Both the 2005 Hurricane Katrina and the 2003 Northeastern Power Blackout were classified as naturally occurring events. Terrorism is an example of malicious event, resulting from malevolent threats and attacks. Figure 13 classifies the incidents according to the attributes of change. The 2000 attack on the U.S.S. Cole is an example of an exogenous terrorist attack [232]. While docked at Aden harbor for a fuel stop, a small craft approached the port side, where explosives were molded against the hull of the boat. The resulting blast caused a large gash in the ship's port side, hitting the ship's galley. Severe flooding occurred, however damage propagation eventually went under control, with a death toll of 17 sailors, and 39 others injured. The 1988 Pan Am flight 103 bombing is an example of an endogenous malevolent attack. While not strictly endogenous, it was a man-made terrorist bombing attack,

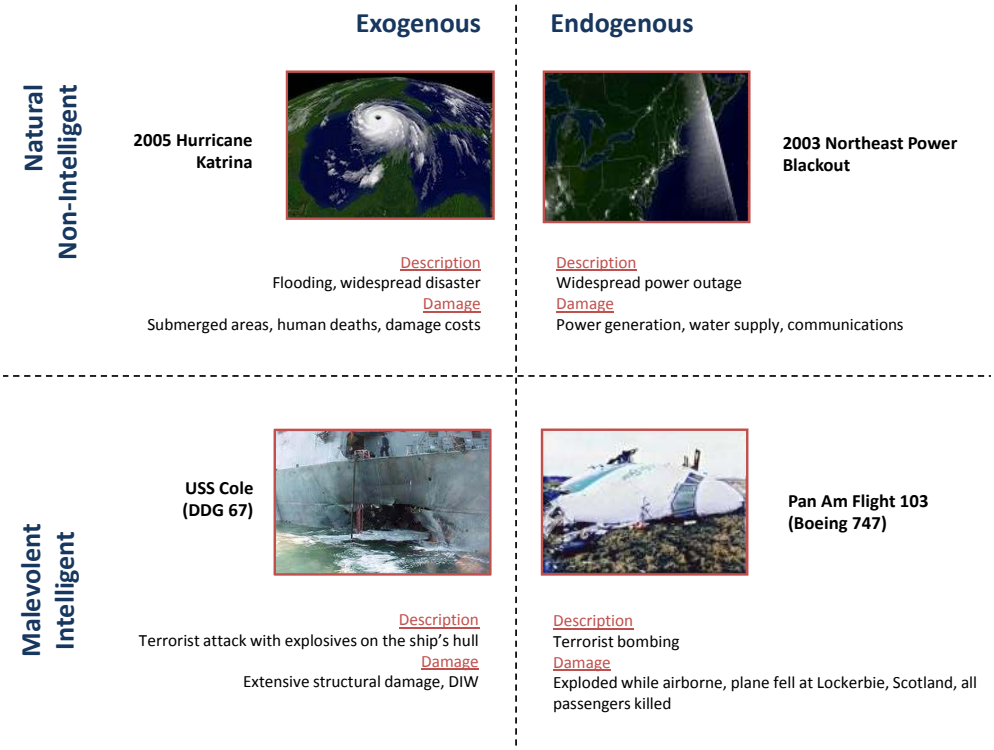


Figure 13: Historical attacks and disasters

which resulted in 270 fatalities [172].

Observation 1.8: Understanding the basic attributes of change, is necessary to further understand, classify and analyze the impact of emerging threats.

1.3.2 Dependability and safety management

Referring to the historical incidents, the affected systems have all been designed with certain capability requirements. Under normal operating conditions, system capability by-design was at levels, as expected by the mission. However, under extreme conditions of "change", it became very difficult or impossible to ensure the same expected mission capability. In that regime, it is asserted that system dependability is what determines the overall system effectiveness. Both system capability and dependability are inherent by design, yet the system's response under extreme change is up to how dependable it proves to be, and this is what also allows capability to

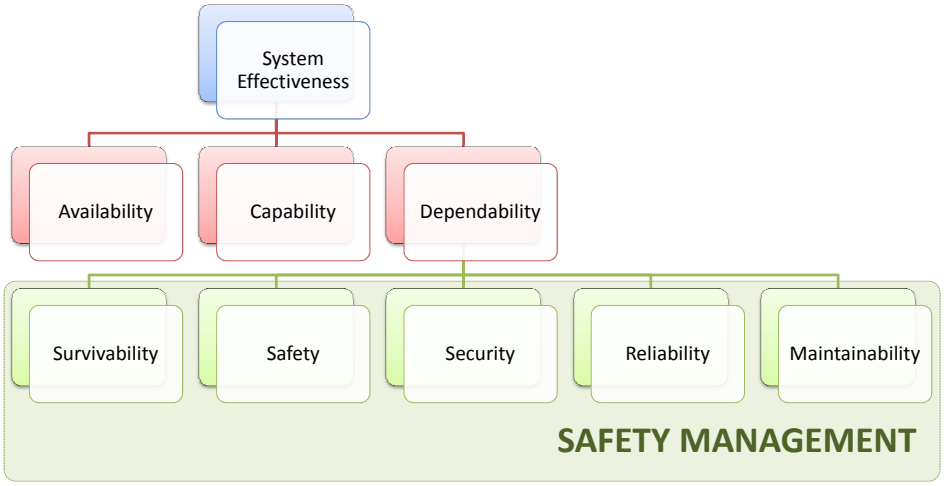


Figure 14: Dependability and safety management

manifest itself. System availability is linked to real time logistics during change, but it is indirectly still determined by dependability. Based on this frame of reasoning, dependability is strategically selected to be brought into main focus in improving system effectiveness through design, for the entire body of this research work.

Dependability is the branch of effectiveness that is directly linked to safety management, as illustrated in Figure 14. *Safety management* is the field of safety engineering that investigates accident related system instabilities with associated hazards, and seeks to propose safety requirements and solutions in order to control system and sub-system operation performance. But before taking a step further, one needs to consider the meaning of system safety under this context.

In 1968, Jerome Lederer, the director of the NASA Manned Flight Safety Program for Apollo defined system safety as [140]:

"System safety covers the total spectrum of risk management. It goes beyond the hardware and associated procedures of system safety engineering. It involves: attitudes and motivation of designers and production people, employee/management rapport, the relation of industrial associations among themselves and with government, human

factors in supervision and quality control, documentation on the interfaces of industrial and public safety with design and operations, the interest and attitudes of top management, the effects of the legal system on accident investigations and exchange of information, the certification of critical workers, political considerations, resources, public sentiment and many other non-technical but vital influences on the attainment of an acceptable level of risk control. These non-technical aspects of system safety cannot be ignored."

Lederer's definition defines safety in a broader spectrum, which not only includes the system as hardware, but also all human and non-human factors regarding system design, operation, policies and procedures, as well as management in all applicable levels.

From a behavioral point of view, system safety is simply known as the "sum of all accidents that do not occur" [111], or that a system is safe if there are no accidents affecting its normal operating conditions, presuming that the only operating risks would always result into a certain set of emerging accidents. In another more generalized version, safety is described as "the state of the system at which nothing unwanted happens" [111]. On the other hand, loss of safety can emerge without the occurrence of anything that might be unwanted, in particular when safety refers to an organization that may include hardware, software or human personnel[62]. Under the previous definitions, safety is represented by a state variable that marks the presence of accidents, or total freedom from them.

But reality indicates that safety is not a binary state representation, thus more states associated to system safety can be found. Except for full accidents or losses, it is understood that partial losses are responsible for different levels of safety, thus Leveson has extended her definition of safety to the "freedom from accidents or losses". Under these premise, safety is defined in terms of acceptable loss [140], and is quantitatively expressed in the form of a nominal safety target (referring to a performance

measure, or utility function). Under this view of safety, it is no longer a discrete state variable, but it takes the form of a continuous loss function, defined as the difference of the system's response under normal operating conditions, minus the degraded performance response [140]:

$$V_{loss} = V_0 - V_{degraded} \tag{2}$$

A third remark points out that safety is *dynamic*. It is not only depending on reliability of static parts, but safety also results as the outcome of complex processes [258]. Accidents occur when external disturbances and dysfunctional interactions between system components create a situation that is out of control. Under this perspective, safety can be viewed as a *control problem* [141], [183], and the mission of safety management is to control system and sub-system process performance, under the effects of operational risk and mission uncertainty.

1.3.3 Safety management concepts

Except for system safety, other major safety management concepts, are system security, reliability, and survivability (often consisting of susceptibility, vulnerability or recoverability). With these concepts as the basis, safety engineers are expected to apply a portfolio of common techniques, in order to ensure and demonstrate that a design is safe. In general, they perform fault analysis studies, and propose safety requirements in design specifications. Safety management techniques are organized under risk identification [126], assessment and estimation [129], as well as under reliability engineering [267].

Risk is a key metric for safety management [12]. The risk of experiencing an accident is linked to safety as a means of operational uncertainty quantification [174]. Risk is typically measured as the probability of a certain set of events occurring, originating from faults and subsystem or system failures [127]. For large scale systems, complexity is a major factor of increasing operational uncertainty and risk [85]. Conditions

leading to threats, hazards and failure risks, either external or internal can emerge between subsystems [100], due to challenging mission expectations or changes in the system's environment [155], [111]. Typical behavior of a complex system is nonlinear, nondeterministic, and possibly chaotic, especially for systems with an increasing number of interactions and subsystem connections [38]. Increasing complexity is also a consequence of extensive usage of revolutionary technology solutions [140]. The appearance of new hazards is a common risk factor, especially as more revolutionary technologies and solutions are introduced for mass consumption with a continuously decreasing average time of conversion of technical discovery into commercial product, thus resulting in technologies that are at low readiness levels [139].

Risk identification, along with risk prevention and mitigation is one of the most common techniques within safety management. Risk identification examines the origins of faults and failures that might become hazardous and provides a relative importance scale for reducing the number of most significant risk factors that can affect system safety to a finite set. For effective risk identification, it should be understood that any choice of technology carries with it possible worst case scenarios that must be taken into account in any implementation or policymaking decision [25]. The most common risk identification techniques are:

- Common cause failure (CCF) analysis
- Fault tree analysis (FTA)
- Failure mode and effect analysis (FMEA)

Reliability engineering is concerned primarily with failures and failure rate reduction. With this approach to safety, the main focus is concentrated on failure as the cause of accidents. The events leading to an accident may be a complex combination of equipment failure, faulty maintenance, instrumentation and control problems, human actions, and design errors [215]. Reliability engineering uses a variety of

techniques to minimize component failures and therefore complex systems failures caused by component failure, including parallel redundancy, standby sparing, built-in safety factors and margins, screening, and timed replacements [184]. While these techniques are often effective in increasing reliability, they do not necessarily increase safety. Accidents may be caused by equipment operation outside the parameters and time limits upon which the reliability analyses are based. Therefore, a system may have high reliability and still have accidents.

1.3.4 Associating safety management concepts

It is a common concern to clarify similarities and/or differences in safety management concepts. The association between safety and reliability has been briefly discussed, yet one may wonder how system security and survivability fit in the big picture. There are plenty criteria to follow, for the purpose on drawing boundaries of each concept's relevance and applicability. One possibility is to create a taxonomy based on combinations of type (natural, non-intelligent, or malevolent, intelligent threats) and origin (endogenous or exogenous) of disturbance, not unlike how the historic incidents of Figure 13 were presented. Based on threat combinations, a 2D schematic of relevant safety management concepts is constructed, also marking overlapping relationships as a Venn diagram and is presented [190] in Figure 15.

If safety is viewed as freedom from accidents or losses, then it refers to either endogenous or exogenous threats, which result in naturally occurring accidents [140]. *Reliability* on the other hand is the probability that a component will perform its intended function for a prescribed time and under stipulated environmental conditions [140]. It is assumed that reliability refers to endogenous and natural non-intelligent disruptions, but still contributes to system safety. Effects of maintainability, aging and deterioration are also effects that are considered while assessing reliability.

However, safety and reliability are not the same. System safety is viewed as an

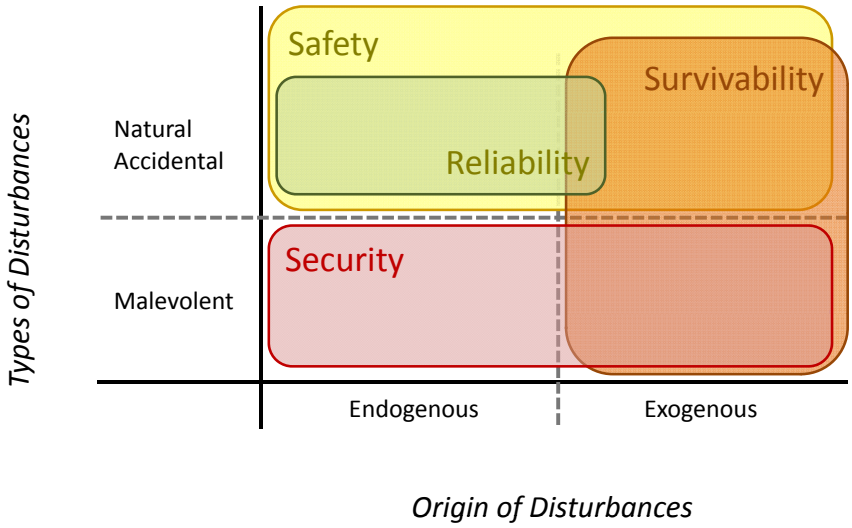


Figure 15: Safety, Security, Survivability and Reliability [190]

emergent property that arises at the system level when components are operating together [216]. Reliability assessment provides measures of the probability of random failures, not the probability of hazards or accidents, as safety is concerned. Reliability analysis uses a bottom-up approach (e.g., FMEA) to evaluate the effect of component failures on system function, while safety requires a top-down approach that evaluates how hazardous states can occur from a combination of both incorrect and correct component behavior, such as proper behavior of a component at an improper time or under the wrong environmental conditions. High reliability numbers do not guarantee safety, and safety need not require ultra high reliability.

In contrast to safety and reliability, system security is focusing on intelligent, intended malicious actions, either endogenous or exogenous. Security is a system property that implies protection of the informational, operational, and physical elements from malicious intent [136]. A secure system should be under adequate protection against losses, system performance degradation, in accordance to requirements imposed by local government or agency regulations. Except for its applicability to standalone entities, such as physical devices and computers, security applies also in

networked systems, privacy and information, as well as national infrastructures or operations. Security can be assessed for either endogenous or exogenous threats, yet it is restricted to actions that affect normal operating conditions, system integrity and durability.

Survivability is more relevant to military engineers [18], with definitions and background that is based on aerospace applications. Survivability has also proliferated in other engineering fields, such as naval or merchant ship design, IT support systems and networks [73], or in some civil engineering applications. Survivability also applies in science based disciplines, such as biology, computer science, systems network theory [134], etc.

Survivability depends on system susceptibility, vulnerability and recoverability. Susceptibility [16] is the probability that the system experiences a direct hit or secondary hit effects through an attack by its environment. Susceptibility is an important component of survivability, in the sense that a threat can be entirely avoided and furthermore ensuring that system vulnerability should not be challenged at all. Vulnerability is defined [16] as the conditional probability that the system is killed after it experiences a direct hit or warhead fusing through an attack by its environment.

Survivability brings the emphasis on the system's behavior and recovery mechanisms. A differentiating feature against safety is that survivability assessment usually assumes intended, intelligent and malevolent actions. In that sense, survivability is more closely related to security in that both are concerned with malevolent environments, where intended and intelligent action take place. Given that the majority of threats usually translate in exogenous actions and changes around the system, survivability assessment methods often dismiss endogenous factors.

Observation 1.9: Depending on the change that occurs within the system or around it, different aspects of safety become relevant, yet they all need to be collectively considered under safety management in early conceptual design.

1.4 Looking at the future of Safety Management: System Resilience

One of the greatest challenges in systems engineering is to ensure that large scale complex system are safe for their operators and their environment, while maintaining their mission effectiveness and performance [146]. Acquisition of military systems must conform to safety standards that the government or delegated agencies mandate for certification [57]. However, with the presence of operational uncertainty, there is no definite approach that eliminates operational risks and the presence of system hazards. Indeed, well-known accidents, either catastrophic, such as the space shuttle Columbia [45], less severe, such as the Airbus A380 engine stall [53], or the unintended acceleration incidents involving Toyota vehicles [165], are evidence for vulnerabilities and increased risks, that otherwise safe certified complex systems encounter.

To address risk, current State-of-the-Art (SoA) safety and risk assessment techniques (PRA, FTA, FMEA, etc.) seek to identify operating conditions and faults that may escalate to failures and lead to accidents with catastrophic consequences [220], [47], [57]. To mitigate this risk, safety oriented technologies are incorporated into system designs, for hazard reduction and safety certification [79].

However, industry and government experts suggest that SoA techniques may not be always adequate for assessing complex system safety. For technology-based risk mitigation, low TRL may introduce additional layers of risk, and regarding safety assessment, SoA probabilistic estimates are only effective, when the outcomes of failure events are accurately identified. The latter requires accurate fault identification and accident modeling [108], a total departure from the current reactive basis that safety management is applied on to incidents and risk challenges. Under this approach, a safety measure is usually taken after certain unexpected incidents occur. Moreover, there is a strong reliance on historical information of past incidents for the conventional risk management that employ hindsight and calculations of failure probabilities

[111]. Last, diagnostics are configured to sense and analyze the symptoms of risk, rather than the origins of risk itself.

Safety engineering and risk management is shifting its paradigm from passive, reactive and diagnosis-based approaches towards development of architectures that will explicitly monitor performance and emerging risks and hazards, and autonomously manage safety and survivability through active, proactive and prognosis-based engineering solutions [111]. However, current technology solutions or advanced design methods are not adequate for implementing this new safety vision for safety, while it is necessary to rethink safety assessment techniques for identifying additional sources of risk [111]. The shift in safety management should not be limited to system architecting or sizing, but it should be broader, ranging from the philosophy and understanding of safety, to safety management essentials, such as rethinking of risk, accident occurrence mechanisms and risk assessment.

In response to this need, the safety management community has introduced a new initiative, known as Resilience Engineering [114]. Resilience is an emerging concept that brings new insight regarding the design of more safe and survivable complex systems [48]. Within the concept of system resilience, failures do not necessarily imply a total breakdown or malfunction of a normal system, as conventional safety definitions would suggest. Rather, a failure represents the inability of the system to adequately adapt to perturbations and changes in the real world given finite resources and time [111]. Failure, in this context, is simply the absence of this ability, when needed, or it is a result of the "web of ongoing interactions and adaptations" that characterizes complex systems behavior in the real world [146]. As such, success is defined by the ability of the system to monitor the changing risk profile and take timely action to prevent the likelihood of damage.

Observation 1.10: Current safety management practices are limited in terms of addressing complexity and its resulting effects, as well as understanding failure and

fault propagation. Resilience is a new concept that is addressing these concerns and brings a new perspective in safety management.

System resilience is an emerging concept, originally introduced through a paper published in 1973 in the Annual Review of Ecology and Systematics by C.S. Holling [106]. Holling's paper was titled "Resilience and Stability of Ecological systems", discussing the relationship between resilience and stability. The purpose was to describe models of change in the structure and function of ecological systems, thus resilience was discussed with this class of systems in mind. The definition of resilience in the context of this publications is expressed as:

"Resilience is a measure of the persistence of systems and their ability to absorb change and disturbance and still maintain the same relationship between populations or state variables."

Given that resilience engineering is still a relatively new concept, it is not a surprise, that there are several unanswered questions regarding its theoretical foundations and its applicability in real world applications [211].

In this context, system resilience is defined as a system characteristic. It's a characteristic that contributes to system stability and robustness. Recognizing that resilient systems are possibly more safe or survivable, scientific communities are embracing the concept in order to address safety challenges. Resilience has also proliferated to other disciplines or fields of engineering and science, addressing equivalent issues in system stability [62], robustness [264], adaptability [96], [168] and survivability [192].

In a broader perspective, Madni describes *resilience engineering* as a discipline that is concerned with monitoring organizational decision making with explicit identification and monitoring of risks [146]. Literature search [120] has indicated that the notion of resilience is growing [249] in importance as a concept for understanding, managing, and governing complex linked systems of people and nature [252].

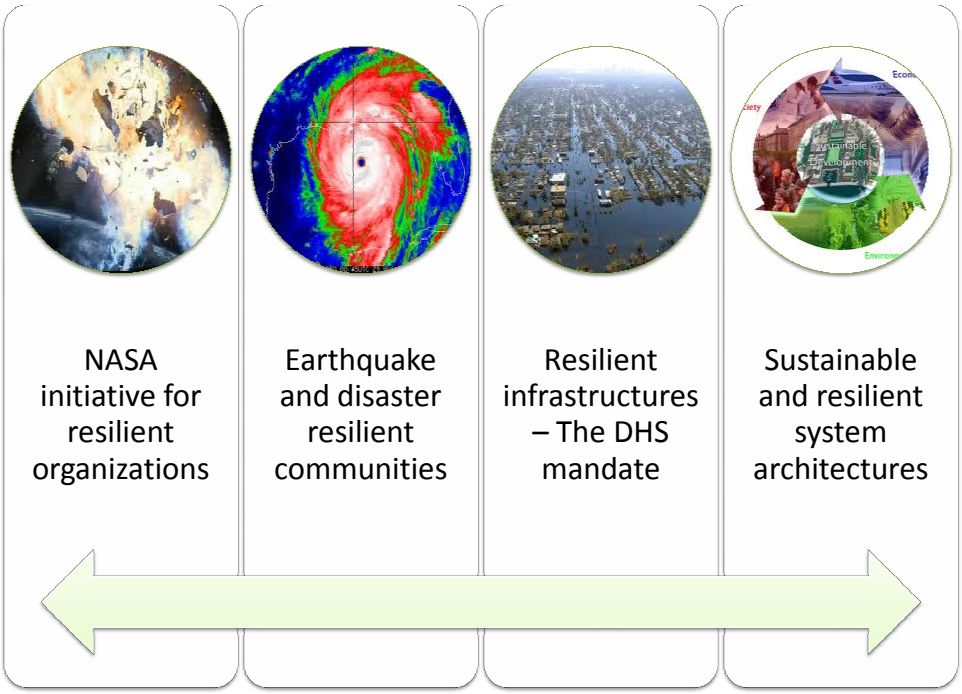


Figure 16: Resilient system initiatives

Four major initiatives have been recently established for addressing resilience in this context, and are listed in Figure 16.

1.4.1 Resilient organizations - The NASA initiative

NASA has been investigating its own organizational decision making practices, as a result of the Challenger and Columbia space shuttle accidents. The importance of such practices, that date back to the post-Cold War policy environment, has been underlined by the Columbia Accident Investigation Board (CAIB) [45]. Attributed to NASA's "faster, better, cheaper" operating principle [265], these accidents have revealed a set of patterns, on which NASA has been basing their decision making approaches[187], and have been documented by the CAIB. These are [265]:

- The drift towards failure as defenses erode under production pressure.
- Past success is a reason for confidence instead of further discovery of underlying risks.

- Adaptation of a fragmented problem solving process that may hide emergent risks.
- Failure to revise assessments as new evidence accumulates.
- Breakdowns at the boundaries of organizational units.

This investigation has demonstrated the inability to balance safety risks with intense production pressure, pushing the organization closer to the edge of the performance envelope without understanding the overall risk increase. These patterns in decision making are not unique to NASA or limited to the Shuttle program, but are generic vulnerabilities that have contributed to major failures across other complex industrial settings.

As an organizational accident, the Columbia experience underlines the need for organizations to monitor their own practices and decision processes, for detecting drift towards safety limits. The target for organizations is to maintain high safety despite production pressure. In this context, a key desire is to accurately assess organizational risk, namely the risk due to insufficient organizational decision making, that may result to drift towards failure boundaries. Safety experts have been advocating for resilience engineering, with its alternative approach in understanding risk, faults and failures in large scale complex systems [145]. As an enabler, the assessment of organizational resilience will consider additional risk factors, such as human performance, and human-machine interaction, and further assist to manage risk proactively. NASA and other high risk organizations could benefit from resilience assessment techniques in balancing competing demands for increased safety with real time pressure for efficiency and production capacity [137].

1.4.2 Earthquake and disaster resilient communities

The NASA initiative on organizational resilience has addressed the problem of organizational decision making practices, as a major contributor of risk in high risk

organizations. Besides decision making and risk identification, organizational resilience depends on the ability of organizations to continue to function in the face of unexpected events. This ability depends on organizational structure, effective management and the resilience of participating systems under high risk or unexpected operations [35].

Historic incidents (e.g the 9/11 terrorist attacks, the 1989 San Fransisco earthquakes and the 2005 hurricane Katrina) could reveal the socio-economic impact of organizational resilience to critical performance measures, such as the length of time that essential services are unavailable and the duration of recovery for the community. The September 11th attacks were responsible for business interruption losses that have by far exceeded the sum of all property losses [2]. After the 1989 San Francisco Bay Earthquake it had been estimated that 50% of small businesses directly affected were permanently disabled, with the resulting job losses significantly impacting the economy of the area [77]. The response to hurricane Katrina and the subsequent flooding of New Orleans, resulted in most part of the city having been destroyed, while governance, law enforcement, medical care, utilities, communications, all entirely failed. The death toll was about 1,500 people, while many thousands became homeless, and billions of dollars of infrastructure has been lost. A million people descended on other communities, often overloading the local systems, while the recovery procedure is still ongoing and is expected to last for many more years [260].

In the wake of such major disasters, recent initiatives have brought attention to disaster and earthquake impact mitigation through more resilient communities. With that objective in mind, the U.S. Federal government [99], affiliated agencies and other independent groups have been supporting the need to evaluate the consequences of risk, while introducing requirements and mandates towards increasing organizational and community resilience [91]. With "Project Impact" in 1997, the

Federal Emergency Management Agency initiated a series of community-based pre-disaster mitigation programs. The goal for this project was to foster public-private partnerships that would undertake hazard and risk assessments, community education programs, and mitigation related projects [241]. Similarly, the Disaster Mitigation Act of 2000, supports mitigation and preparedness planning, offering incentives for disaster mitigation. Other similar initiatives support the development of strategies for disaster resilient communities, while addressing long-term issues of sustainability and quality of life [159]. Because of their potential for producing high losses and extensive community disruption, earthquakes have been given high priority in efforts towards more resilient infrastructures [35]. The civil engineering community is investigating possible approaches on mitigating seismic risk and the potential for future losses [52], through voluntary practices or mandatory policies aimed at reducing the consequences of an earthquake, along with training and preparedness measures.

1.4.3 Resilient infrastructures - The DHS security mandate

The U.S. Federal government has been investigating the concept of resilience, not only for adressing disaster response, but also infrastructure security [99]. In the past, the U.S. government policy towards Critical Infrastructure Protection (CIP) has focused on physical protection [136] and asset hardening. However, recent events, such as the 9/11 terrorist attacks have lead to reconsideration of all past efforts toward physical protection of infrastructure assets. In particular, it was understood that isolated protection is inadequate, since not all disruptive events, natural or man-made, can be prevented, while terrorism has been included as a threat, against which critical infrastructure must be protected, as indicated by two of the first post-9/l1 Presidential directives [36].

The Department of Homeland Security (DHS) assembled the Critical Infrastructure Task Force (CITF) in 2005, for providing recommendations on national policy

and for updating CIP policies to account for unavoidable disruptive events. With the focus on recommendations that would ensure reduction of the consequences of the exploitation, destruction, or disruption of critical infrastructures, the CITF's primary recommendation was that DHS focus on *Critical Infrastructure Resilience* (CIR) as its top-level strategic objective. The recommendation stated that:

"...making resilience the overarching strategic objective would stimulate synergistic actions that are balanced across all three components of risk. Protection, in isolation is a brittle strategy. We cannot protect every potential target against every conceivable attack; we will never eliminate all vulnerabilities. Furthermore, it is virtually impossible to define a desired end state -to quantify how much protection is enough -when the goal is to reduce vulnerabilities."

CIR is concerned with how critical infrastructures absorb, adapt, and recover from the effects of a disruptive event to ensure delivery of critical infrastructure services [251]. It complements the CIP with fostering systems-level investment strategies, recognizing that the stakeholders must bear the costs of resilience through cost/benefit decisions in a changing, competitive environment. The ability to absorb, adapt and recover must be evaluated from a systems functionality perspective, so that proper investment strategies can be planned for the future. [50]. CIR implies a systems approach, one where stakeholders manage both the risks of individual, and the overall system functions well, during a disruptive event.

The DHS National Infrastructure Protection Plan (NIPP) is an initiative that is promoting the resilience of the nation's critical infrastructure [181]. With the shift from CIP to CIR, the federal government has been introducing resilience initiatives to understand what features create resilience in critical infrastructures/key resources (CIKRs). The goal is to build a safer, more secure, and more resilient infrastructure by preventing, deleting, neutralizing, or mitigating any adversary attempts against

the nation's CIKR, while strengthening national preparedness, timely response, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency [50].

1.4.4 Sustainable and resilient system architectures

With the previous initiatives promoting system resilience as an enabling concept in addressing organizational risk, safety, survivability, and security, a fourth resilience engineering initiative brings attention on a non-safety management related objective, that is sustainability of systems and infrastructures [117]. As sustainability goals are formulated and mandated by governments and environmental protection agencies, the development of sustainable systems remains challenging, due to the broad range of economic, environmental and social factors that need to be considered across a system's life cycle [83]. Previous work on sustainable design has focused largely upon ecological efficiency improvements [251]. Examples of this philosophy include material and energy intensity reduction, as well as waste conversion into valuable secondary products.

For pursuing sustainable development, a systems approach is necessary for the design of industrial product and service systems. However, conventional systems engineering approaches primarily rely on disruption anticipation and resistance, without considering vulnerabilities to unforeseen factors. With time constraints and limited cognitive and physiological resources, there is enough room for increasing risk and hazards that could allow for accidents to occur. In the presence of environmental uncertainty and risk, sustainability challenges may be successfully addressed, when design for inherent resilience becomes a primary goal. Based on this initiative, the concept of resilience can be extended to ecological systems, implying cultural adaptability in the face of external disruptions, either as regulatory reform or climate change. Under this approach, fundamental properties such as diversity, efficiency,

adaptability, and cohesion are the building blocks of supporting system resilience, in both engineered systems and the larger systems in which they are embedded.

Observation 1.11: The concept of resilience is gaining interest from diverse engineering communities that have been exploring its applicability. From organizations, infrastructure and sustainable environments, to large scale mechanical, electrical and civil applications, resilience is becoming part of the future in safety management practice, in the form of Resilience Engineering.

1.5 Research objectives and goals

The significance of national security relies upon the fundamental desire for economical and social stability. To preserve and uphold national security, the Armed Forces have been mandating the development and acquisition of more capable systems. System capability requires system safety and survivability, under the presence of operational uncertainty and risk. From a collective standpoint, these requirements lead to the need for more effective systems, as previously outlined by Observations 1.1 to 1.5.

System effectiveness is indicative of the system's total capability of achieving its current mission's objectives and reflects how well can these objectives be achieved. Thus, through capability, system effectiveness is driven by uncertainty in mission operations and the threat environment, as well as by the system's internal complexity and fragility [125]. Besides mission logistics and by-design system capability, a key enabler for effective military systems, is system survivability (Observation 1.6.1) [182]. This observation is also confirmed by the Navy's vision for their future combatants, as expressed by the IEP concept and their direction with the DDG-1000 [143], [43]. Aligned to the Navy's requirements, the IRIS initiative commands for more effective systems through increased situational awareness and system survivability, enabled by automation, reconfigurability and intelligent control architectures [115].

However, the challenge of designing next-generation ship systems [259] that would

meet the Navy's goals for system effectiveness, environmental compatibility, and reduced cost has grown to the point that traditional design methodologies are becoming ineffective [33]. Under the direction of improving survivability, a major shift may be necessary on how survivability-based design is applied. There are concerns that *a posteriori* survivability design approaches may increase development and acquisition costs, add unnecessary complexity and introduce additional design uncertainty, thus challenging the overall effectiveness of resulting designs. In a broader perspective, this issue becomes more critical, as complexity is further increasing with larger scale systems, or by considering process-related obstacles, such as demanding analysis requirements for complex system, large number of objectives and constraints to be evaluated, and the multitudes of uncertainty sources that appear in current design problems. Earlier literature search has indicated lack of cohesive and widely accepted methodologies to address system effectiveness and survivability as design attributes in the early conceptual design process [218]. As Observation 1.6.2 reaffirms, there is a research opportunity for the development of conceptual design methodologies that introduce survivability as on objective function.

Observations 1.6.1 and 1.6.2, along with Observation 1.7 that relates to affordability concerns for future naval systems, lead to the main objective of this research, that is expressed as:

Objective 1 (Main): Invest towards conceptual design methodologies that improve system effectiveness through increased survivability.

The goal of this research objective is to produce effective designs that reduce operating costs, while improving safety, security and overall survivability. In accordance to earlier discussions and summary of observations, the basic steps of establishing this research direction are presented in Figure 17.

At the same time, as Observations 1.8 and 1.9 suggest, current survivability-based

Figure 17: From observations to research objectives

design procedures may not be adequate in addressing new threats, challenges, demands, and opportunities. Moreover, revolutionary architectures and configurations also advocate for new approaches in survivability-based design. As Observation 1.10 has stated, this new approach must address dynamic phenomena due to complexity (emergent behaviors), be capable of better predicting the impact of changing requirements or environmental conditions, and consider risk and operational uncertainty in a whole new way. Thus, as Observations 1.10 and 1.11, recommend, resilience engineering is a new approach that seeks to address these issues, and its underlying philosophy must be taken into account during the formulation of advanced survivability-based design approaches. The second objective of this research is to:

Objective 2: Follow the vision of resilience and investigate options on how resilience engineering can be implemented in advanced design methodologies with safety management concepts as objective functions.

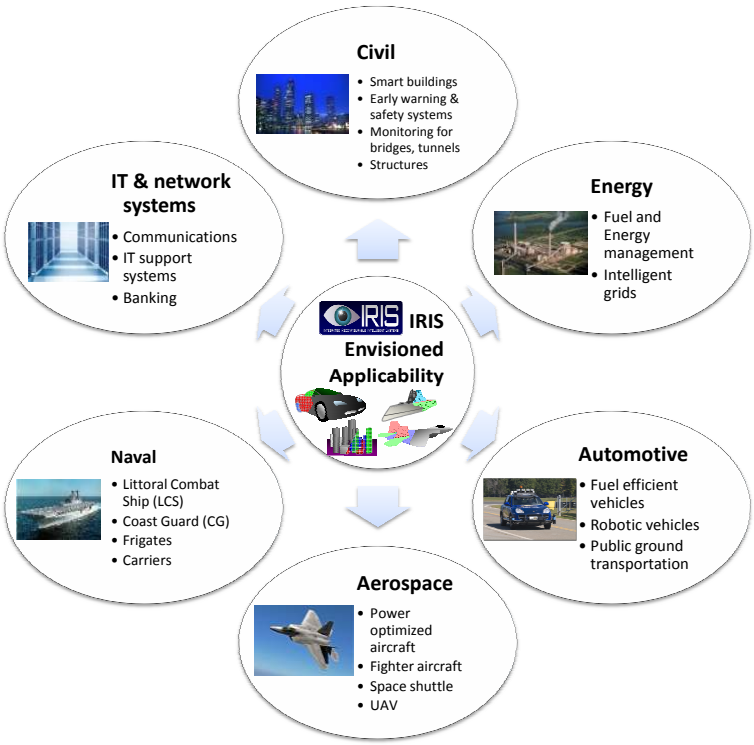


Figure 18: IRIS envisioned applicability

The goal of this objective is to infuse the premises and visionary directions of resilience engineering into advanced design methods for safety management. These efforts could extend beyond survivability-based design, and find their way on a diverse set of applications, such as naval systems (destroyers, frigates and carriers), aerospace or space vehicles (fighters, UAVs, satellites and the space shuttle [14]). The philosophy of resilience could proliferate beyond the system level, to component or network level, or to higher organizational levels. (e.g., the Smart Grid [89]). In conjunction with the IRIS initiative, resilience-based design techniques could benefit a large variety of applications, as listed in Figure 18 a summary of the IRIS envisioned applicability is provided.

1.6 Dissertation structure

This dissertation is organized into seven chapters. With Chapter 1, there has been an introduction to the problem from a global, less concentrated perspective. The need for more effective, capable and survivable military systems has been discussed from a high level point of view, namely from a national, societal and military-oriented perspective. At the same time, a first introduction on the relevant scientific concepts has been included, spanning from system safety, survivability and looking at the future of safety management, through the emergence of resilience engineering.

Chapter 2 aims on providing a process for a clear problem statement, based on an comprehensive and exhaustive background investigation for all problem related disciplines. This has been an interdisciplinary effort, ranging from various theoretical formulations and considering a diverse set of applications, to promote better understanding of the practice. The key topic is the investigation of safety management, in the form of safety, and survivability-based design methodologies, for military and civil large scale complex system applications. This investigation has returned a great wealth of technical background information, regarding definitions of key concepts (safety, survivability, reliability, resilience, etc.) and metrics. With a better theoretical and technical understanding, the ground has been prepared for a concentrated problem statement.

With better understanding of the design capabilities in safety management, Chapter 3 is advocating for concentration on assessment techniques, as being a crucial step for safety-based design. State-of-the-Art (SoA) approaches that are currently used by the government, industry and academia for benchmarking system safety, survivability and resilience assessment have been explored and presented. For all methods and techniques identified, under this research effort, comparative evaluation of SoA techniques follow, with focus on the benefits and detriments of each technique, in comparison to others. This evaluation lead to a list of major technical challenges

that are identified and will assist in formulating the clear research directions for this dissertation, in the form of the Research Questions.

In Chapter 4, the Research Questions for this work have been defined, in accordance to the gaps in SoA approaches. Preliminary knowledge on the derived research topics, as well as engineering intuition from similar types of problems, have resulted in a hierarchy of testable and falsifiable research hypotheses that will be further tested , as part of this dissertation's grand experimentation plan.

Chapter 5 moves along the path of establishing a resilience assessment framework. Under the guidance and simplicity of a small scale system model to play the role of a canonical experiment for method development, the Resilience Assessment Technique is developed, tested and demonstrated. The canonical problem configuration includes a multiple-spring-mass-damper system, with a single degree of freedom, which allows for integration of rule-based, feedback controller, that ensures good system health, and overall mission capability.

Chapter 6 is focusing on the demonstration of the resilience assessment technique on a naval system application. The baseline naval system is a small scale naval operations architecture, that includes an integrated power and cooling system. A perfect response controller is part of the facility, which allows for system response prediction, under the presence of leaks on the network, as part of the presence of operational uncertainty.

Chapter 7 concludes with the key findings and lessons learned from this work. It also suggests a number of possible improvements and it recommends the future research directions that could be take to further investigate the problem of system effectiveness.

CHAPTER II

BACKGROUND: EXPLORING OPTIONS IN SAFETY MANAGEMENT FOR IMPROVING SYSTEM SURVIVABILITY

Safety management is the key topic that will drive background exploration through literature search on safety and survivability-based design methodologies. As system effectiveness is the starting concern for the design of future naval systems, the presence of uncertainty and the effects of risk are always present throughout this background search. The goal of the chapter is to expand the scientific knowledge on the field of safety management, while using this knowledge for carving a complete and comprehensive problem statement that is expected to drive this research.

2.1 Safety engineering

Safety engineering is founded on systems theory and systems engineering, and its major objective is to prevent foreseeable accidents, while minimizing the impact of unexpected and unavoidable ones. Safety is not always integrated to the system design process. It is not until the detailed design phase, when requirements for system safety certification are considered, and safety enhancements are introduced. These include modifications on the architecture to retrofit additional safety oriented equipment [81], or the integration of additional technologies that aim towards maintaining safety and survivability [167]. In most cases however, system architectures are seldom designed from the very beginning to seamlessly accommodate all safety considerations.

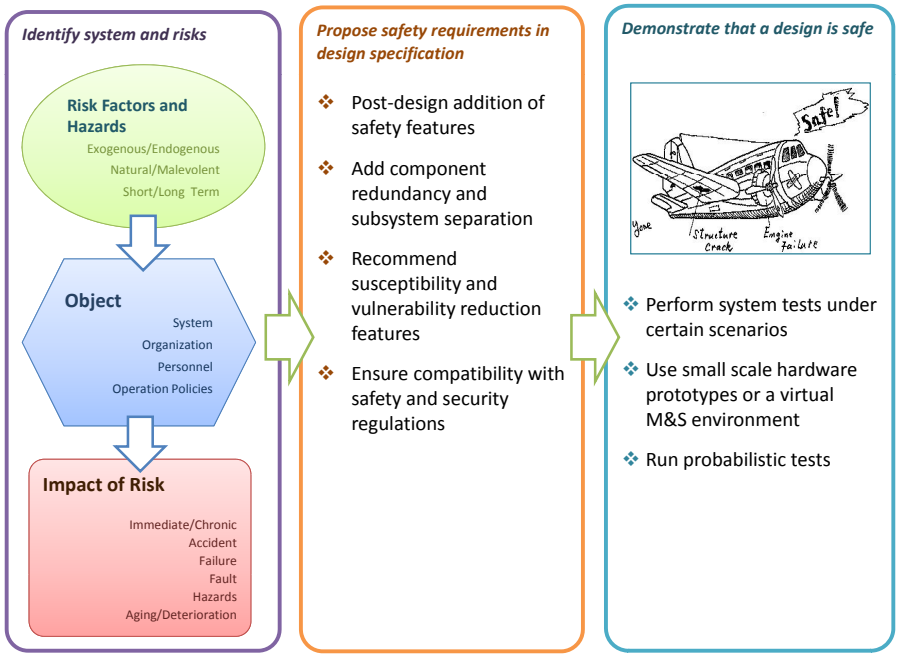


Figure 19: General safety by-design practical procedure

2.1.1 Overview of SoA

Current State-of-the-Art (SoA) methods in safety engineering rely on risk identification, risk assessment, safety management for hazard control or elimination, and risk-benefit analysis [140]. As part of the design approach, the acceptable level for risk is selected, while accounting for other possible sources of risk that may emerge. Risk assessment is vital for strategic decision making, in selecting safety oriented design improvements (e.g. component redundancy, separation, advanced safety technologies). Risk-benefit studies and prototype testing indicate how further must the designer proceed with safety improvements. A general overview of current practical approaches in safety by-design, is pictured in Figure 19.

System safety is becoming a core value in systems engineering [223], through emphasizing on built-in safety characteristics. To address safety as an early design objective, several risk and reliability-based design methods are available for different

engineering applications. Safety by-design is mainly enabled by *Reliability Engineering*, which is traditionally focusing on improving system reliability through advanced structural design and manufacturing techniques. One of the most prominent techniques is *Reliability-based Design Optimization* (RBDO), which concentrates on long term reliability and system health [267], in operating environments with known disturbances. Furthermore, *Robust Design* is a technique for improving system quality and performance under varying external factors. Despite its focus on quality of service, it implicitly does address safety concerns in early conceptual design [230].

Fault generation and propagation models, as well as accident mechanism investigation are key procedures within safety engineering. Most accidents, failures and malfunctions result from losses in performance, security and system integrity, under the presence of threats and environmental hazards. In order to link the impact of a threat to performance degradations and to resulting faults, threat characterization is necessary, for obtaining the complete picture of how the system becomes exposed, vulnerable and eventually affected by their presence. Common accident investigation techniques are *Fault/Event Tree* analysis [78] [220], and the *Common Cause Failure*(CCF) analysis [185]. Advanced techniques rely on more accurate accident and damage prediction through physics-based Modeling and Simulation (M&S) [30].

2.1.2 Applications in safety engineering

Safety by-design techniques have been applied to a wide range of system types and configurations [147]. The State-of-Practice (SoP) in safety-based design techniques is found in military and civil applications for aerospace or naval systems, while extending to energy generation and automotive systems. the most commonly applied techniques for these systems are presented in Figure 20.

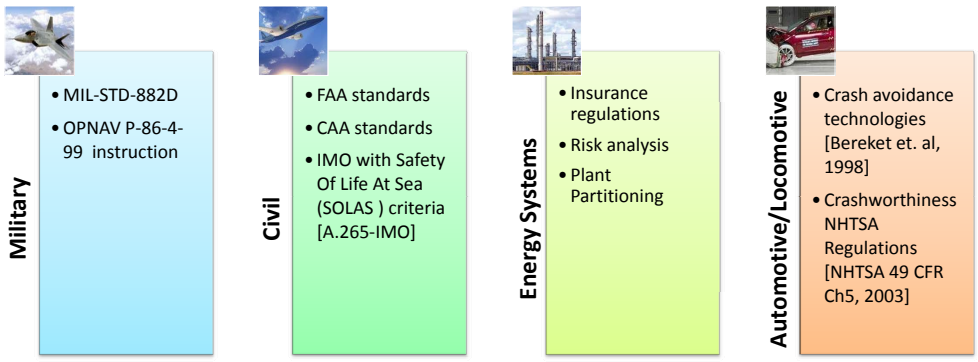


Figure 20: Safety-based design SoA applications

2.1.2.1 Defense and Military systems

As an independent discipline, system safety was introduced for military aircraft, immediately after World War II. Due to the increased number of accidents at the time, engineers were advocating that safety must be designed and built into aircraft just as are performance, stability, and structural integrity [141]. In the following years, safety engineering was recognized as discipline through ballistic missile programs [141]. Similar system safety programs became popular within the Army and later with the Navy.

During the early years of safety engineering, each designer, manager, and engineer was assigned responsibilities for monitoring safety, while safety management was executed as a "fly-fix-fly" approach [141]. With limitations in prototype testing, the DoD realized that this approach was expensive and inefficient, while being dependent on risk analysis methods that use past historical data. In 1966, the DoD issued a directive for initiating system safety programs, recommending hazard analysis techniques. The goal was to prevent accidents before they occurred and suggest that operational safety practices be integrated to technical analysis, design and management approaches of the time.

Safety is now a major concern in military system development, as well as space

programs (e.g. the Space Shuttle [14]). The MIL-STD-882 military standards document was first issued in 1969, introducing minimum system safety requirements, throughout the life cycle for any DoD system [57]. Besides new system development, the directive also governs upgrades, modifications, resolutions of deficiencies, or technology development. MIL-STD-882 is the first practical step for a systematic approach towards managing the acceptable mishap risk, through hazard analysis, risk assessment, and risk management [57]. A summary of the recommendations for implementing system safety is shown below in Figure 21.

The U.S. Navy has also introduced policies and procedures for safety monitoring and implementation, which are heavily based on the MIL-STD-882, and they are complemented by DoD Instruction (DODI 5000.2), by the Secretary of the Navy Instruction (SECNAVINST 5000.2D) and the Navy System Safety Program Policy [40]. Their recommendations address critical safety issues around noise & vibration, ergonomics/human factors, ventilation & heat stress, electrical equipment and radar operation [167]. The policies seek to identify potential hazards during the design process, manage safety threats to program viability and cost, track and resolve potential hazards and reduce hazards that were overlooked during the process [171]. In the system level, the benefits concentrate on operational readiness, health monitoring and support, and life cycle cost reduction for all acquisition programs, over the entire program life cycle.

2.1.2.2 Civil transportation systems

The Federal Aviation Agency (FAA) requires that no Hazard Class I or Class II conditions for single system component failures are acceptable [82] for new aircraft certification. Class I (Catastrophic) Hazard Level considers of failure conditions that would prevent continued safe flight and landing, while Class II (Hazardous) Hazard Level includes of failure conditions that would reduce the capability of the airplane

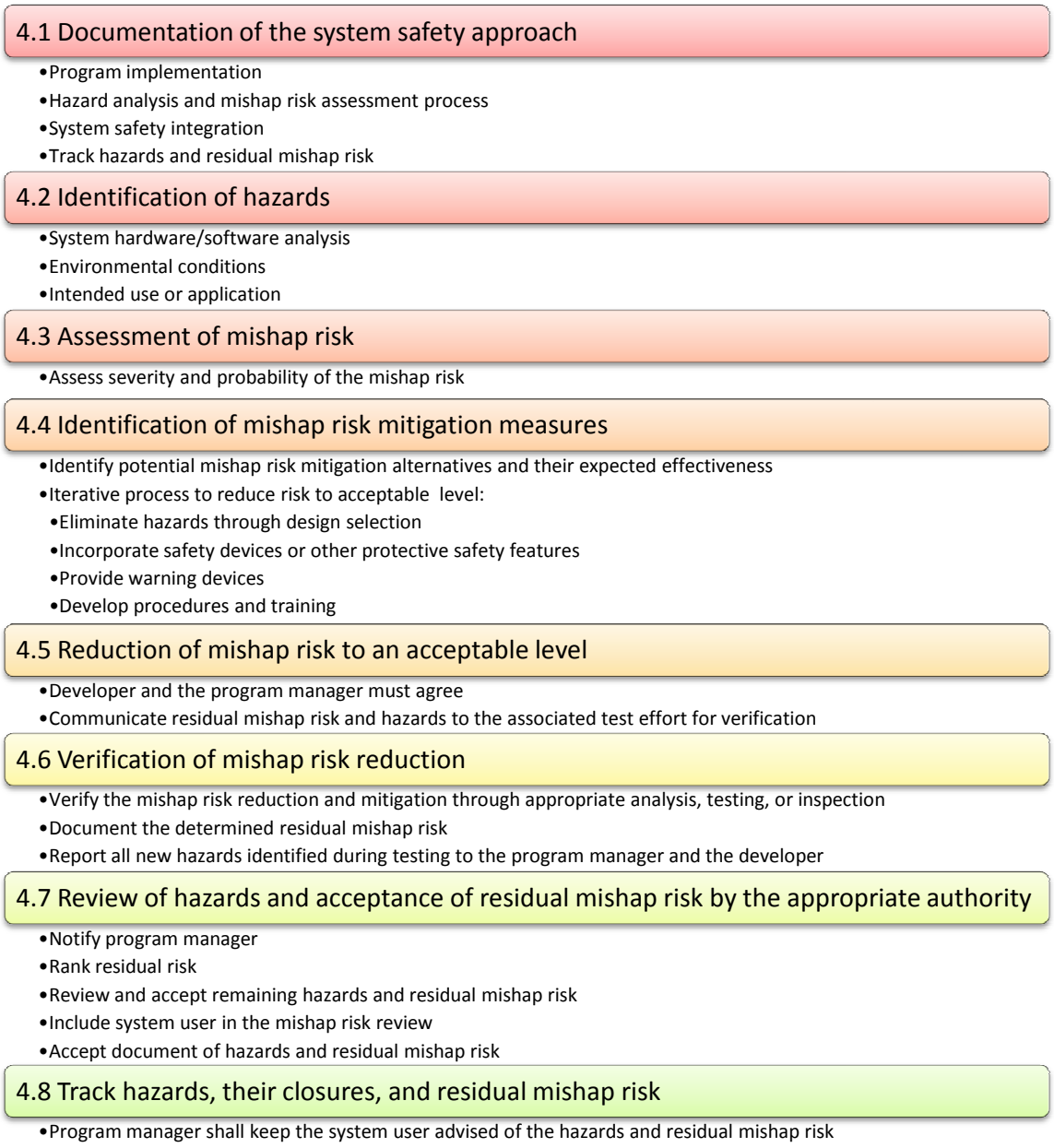


Figure 21: DoD military system program safety requirements and recommendations [57]

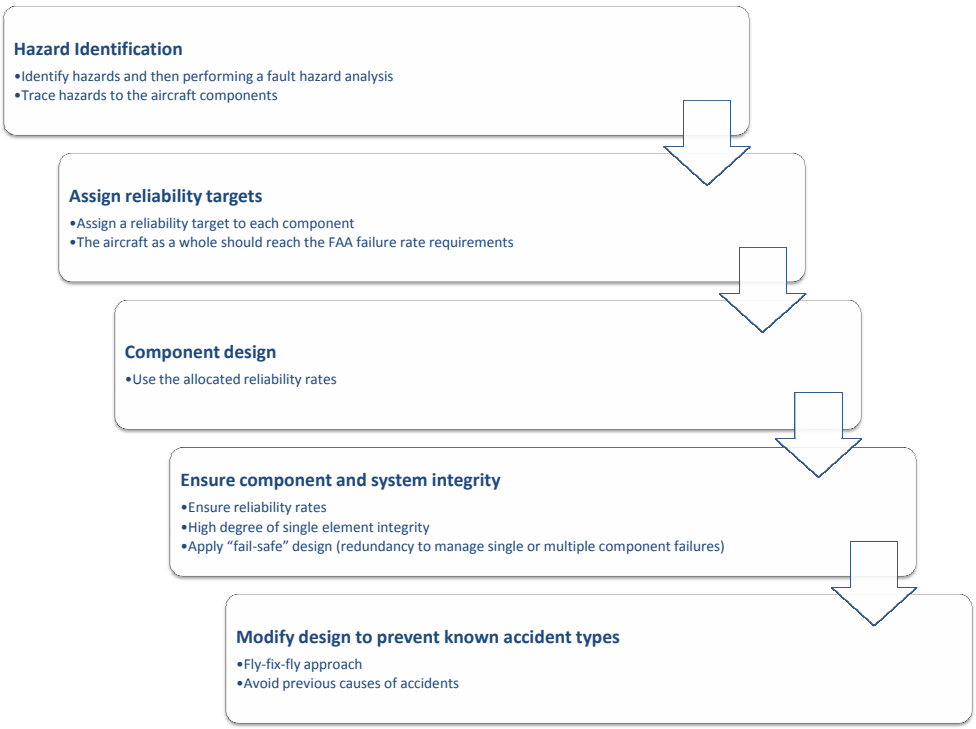


Figure 22: SoA aircraft safety-by-design approach [141]

or the ability of the crew to cope with adverse operating conditions to the extent that there would be a large reduction in safety margins or functional capabilities. As a possible interpretation of the FAA's safety policies, Figure 22 outlines a process for ensuring that a system is safe by monitoring and improving component reliability rates.

In Europe, similar policies have been formulated by the Civil Aviation Authority (CAA), mainly addressing system or component failures due to natural unintentional conditions. Understanding the potential for improving the aircraft's natural resistance to detonation of improvised explosive devices and IEDs in cargo areas, the CAA is focusing on aircraft vulnerability. That includes the effects mitigation of explosive devices in asymmetric threats or other acts of sabotage towards the aircraft's fuselage structure and other vital systems [42].

Similarly to the FAA and CAA, the International Maritime Organization (IMO)

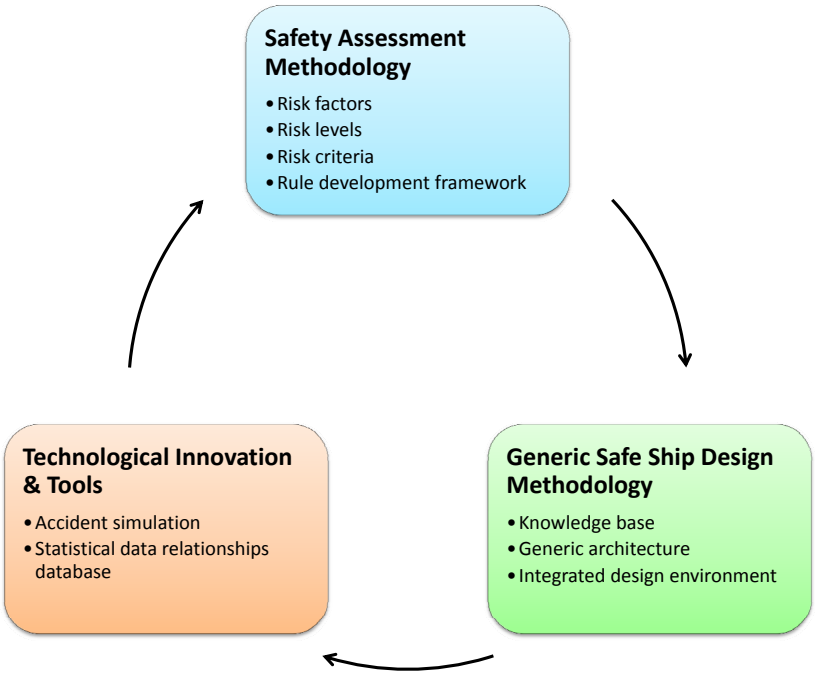


Figure 23: IMO philosophy for safety-by-design [204]

is the responsible authority on formulating safety regulations and recommendations for passenger transport and merchant ships. Except for safety assessment and management procedures, IMO has introduced regulations (A.265 (VIII)) for ship survivability. IMO has been working on probabilistic frameworks for safety assessment, involving prescriptive (regulative) or multi-level, performance-based approaches. Under this direction, ship safety is founded on five main thrusts: structural safety, ship and cargo survival, passenger survival, seaworthiness and fire safety [204]. To address these thrusts, the IMO has established four related R&D activities, focusing on the development of critical technologies, methodologies, tools and techniques, risk-based frameworks (safety assurance techniques and methodologies), integrated design environments(utilization of advanced design techniques) and the overall philosophy on designing for safety. These R&D areas, have become the basis for the formulation of a template for risk-based assessment, technology development and infusion to support safety-by-design, as explained in Figure 23.

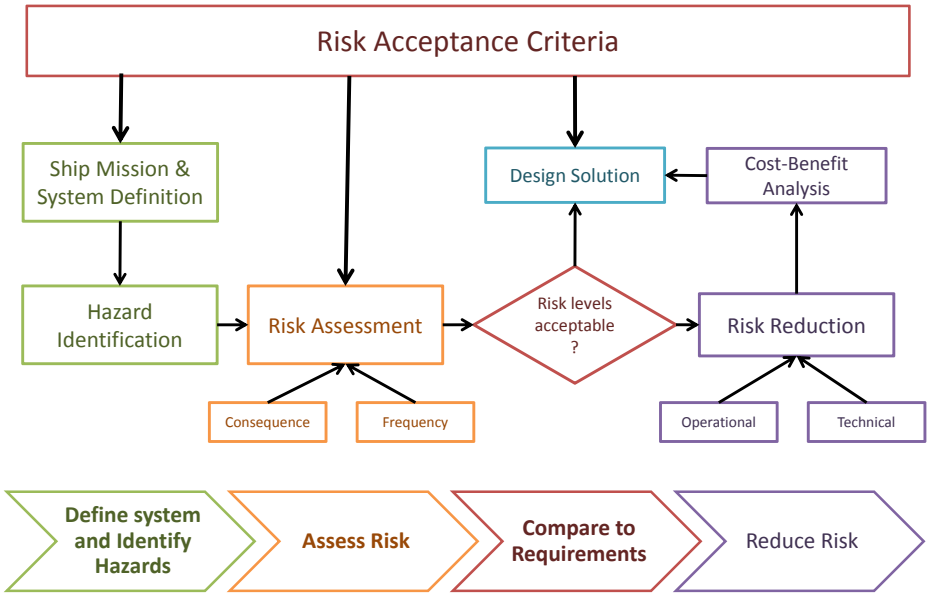


Figure 24: EURORO risk-based procedure for safety design [204]

Under the EURORO approach, a key element of the design approach, is the risk analysis and assessment technique. Risk analysis may require computational tools for predicting collision, grounding, large scale flooding, cargo shift, extreme load effects, fire and passenger evacuation [204]. With IMO's EURORO as the basis, agencies have been formulating risk-based procedures for safety by-design. An example is presented in Figure 24, with a EURORO-compatible approach that is implemented in four basic steps [173]:

1. System and hazard identification.
2. Risk assessment.
3. Comparison to requirements.
4. Risk reduction approaches.

The first step is to identify all possible hazards that increase risk of failure, e.g. such as flooding and fire related hazards [173]. By monitoring and analyzing the frequency and impact of hazards, the risk of malfunctions or failure can be assessed. Risk

assessment relies on risk analysis techniques, such as the Fault Tree Analysis (FTA) [78] and the Failure Modes and Effect Analysis (FMEA). For FMEA in particular, it is necessary to analyze the system's behavior, either through processing of historical information or advanced simulation-based techniques. Simulation techniques rely on computational models that predict system degradation in intermediate performance stages from normal conditions to a total system loss [173].

In the next step, the quantitative risk estimates are compared to risk acceptance criteria [204]. Risk criteria are derived by policies and regulations that are set by associated government institutions or delegated authorities. In 1974, IMO established the Safety Of Life At Sea(SOLAS) criteria, which outline the responsibilities of the ship as a system and its occupants, for minimizing the probability of ship or human life loss [118].

As a means for controlling operating risk, technologies and design solutions enhance the system's response in certain emergencies and adversary conditions [47]. With a large set of risk reduction approaches, technology selection will depend on cost-effectiveness estimations, where effectiveness is viewed as the balance between performance and ability to satisfy safety regulations. Returning to safety at sea, an implementation of the risk-based, safety by-design methodology could result in a multi-step procedure, similar to that of Figure 25. Candidate design solutions are evaluated based on their cost-benefit performance, with the viable solutions only thereafter assessed for their effect on other performance factors, such as seakeeping, cargo capacity, operational efficiency, and turnaround time [31].

2.1.2.3 Energy Systems

In conventional and nuclear powerplant design, safety assurance is based on the use of multiple, independent partitions. The goal is to ensure the integrity of each component, as well as that no single failure of any active component will disable any

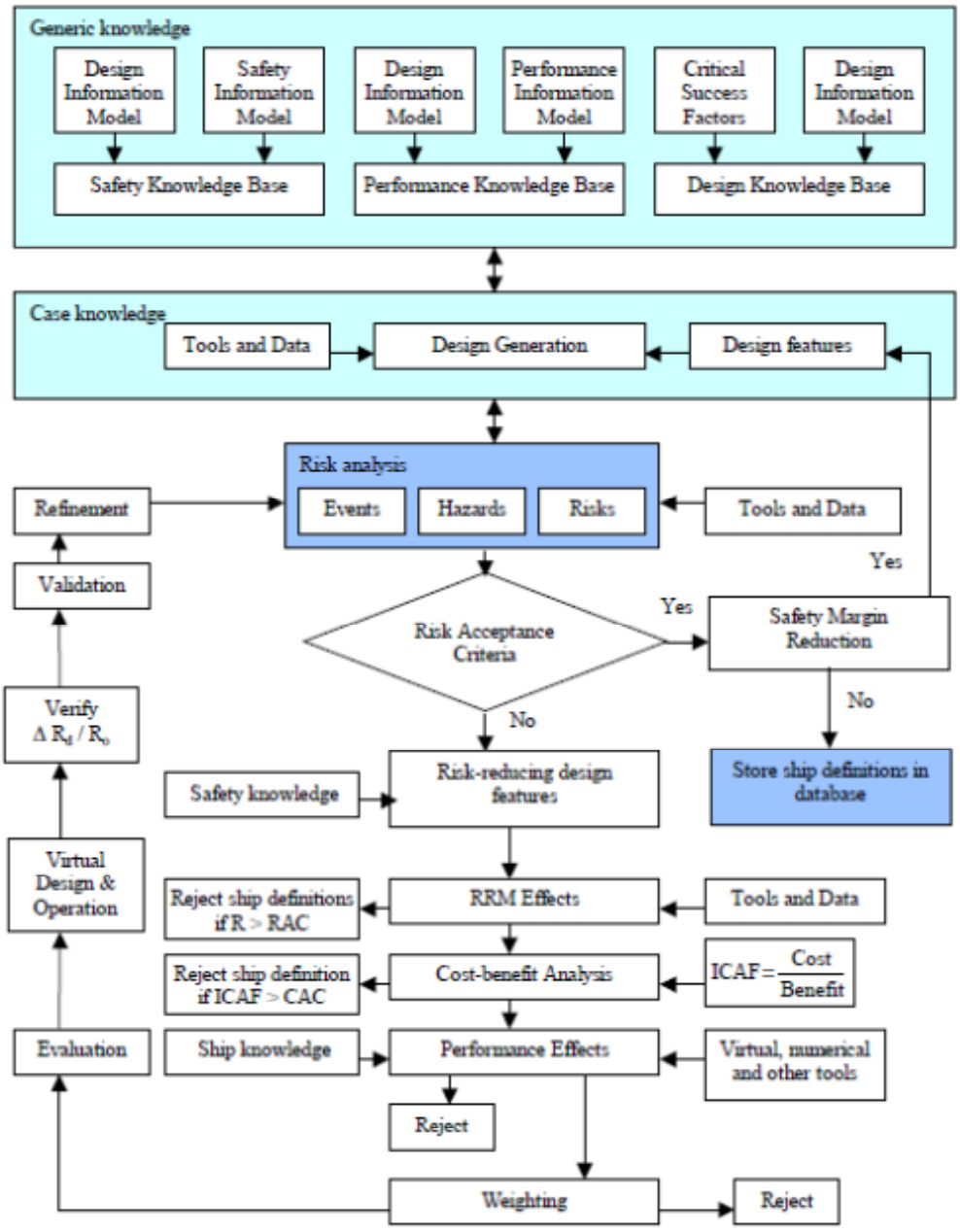


Figure 25: Detailed risk-based procedure for ship safety design [204]

partition [141]. Powerplant certification for safety is based on the identification and control of hazards under normal operating conditions [102], and system shutdown for the investigation of system response to abnormal and unexpected conditions [141].

As part of the design process, safety is not government regulated, but requirements are based on insurance needs. Risk analysis requires a number of scenarios. Scenarios are formulated based on past accident cases, mostly involving operational disturbances, a protection system that fails, and inadequate or failing physical barriers. The main emphasis is on component reliability and protection systems. Risk analysis typically takes place during the late stages of the design process, allowing for any retrofitting of the additional safety equipment that is required for satisfying the certification requirements [141].

2.1.2.4 Automotive/locomotive systems

Automotive safety depends on vehicle crashworthiness, as well as technologies that improve crash avoidance. The National Transportation Safety Board (NTSB) offers recommendations on occupant protection, with emphasis on cabin structural integrity, functional component design improvements, as well as fire detection and suppression systems [166]. Thus, vehicle crashworthiness is another way to express vehicle vulnerability, as recognized by the National Highway and Traffic Safety Administration (NHTSA) [164]. Similarly, vehicle crash avoidance is a measure of susceptibility for ground operated vehicles, which relies on both the vehicle and transportation infrastructure.

Crash energy management methods are the enabling backbone for crashworthiness improvement, while computational (finite element) analysis methods are vital for reducing product development time and cost and satisfying corporate and government crash safety requirements (e.g. NHTSA for frontal, side, rear impact, interior head impact, rear impact, and rollover) [236]. Vehicle crash avoidance relies on

technologies that support collision warning [235], adaptive cruise control and braking. Infrastructure-based approaches focus on intelligent vehicle-highway systems, for instance, monitoring the dynamic conditions that set apart safe from unsafe lane changes [22]. Human factors-based approaches investigate the behavior of crash avoidance systems and their interaction with driver performance [80], e.g. human braking in conjunction to the vehicle's Adaptive Cruise Control (ACC), Forward Crash Avoidance (FCA) systems, and Forward Collision Warning (FCW) [80].

Such technology solutions are relatively new and not developed to their full extent, given the uncertainty as to how situational awareness is maintained and how crash mitigation systems, could seamlessly partner with human activity [121]. Advanced design methods for vehicle crashworthiness concentrate around reliability and system integrity. Under the presence uncertainty, the Risk-Based Design Optimization (RBDO) method is applied to address risk concerns in vehicle safety [267]. With RBDO, a probabilistic constraint can be identified by either the Reliability Index Approach (RIA), or the Performance Measure Approach (PMA) [267]. For vehicle crashworthiness, RBDO is using the PMA, when dealing with vehicle safety-rating scores related to human safety issues, along with response surface techniques for reduced cost of application.

2.1.3 Evaluation of SoA in safety-based design

As observed by the SoA review in safety-based design, system safety is receiving great attention from various engineering disciplines, for civil, aerospace, naval/marine, automotive/locomotive vehicles, as well as industrial and energy applications. Starting from the collection of methods presented in Figure 20, a methods evaluation study has been conducted, in order to identify their strengths, the weaknesses and the opportunities that arise from the SoA. The insights from this study will steer the research efforts towards the necessary direction of improvement. The collected methods have

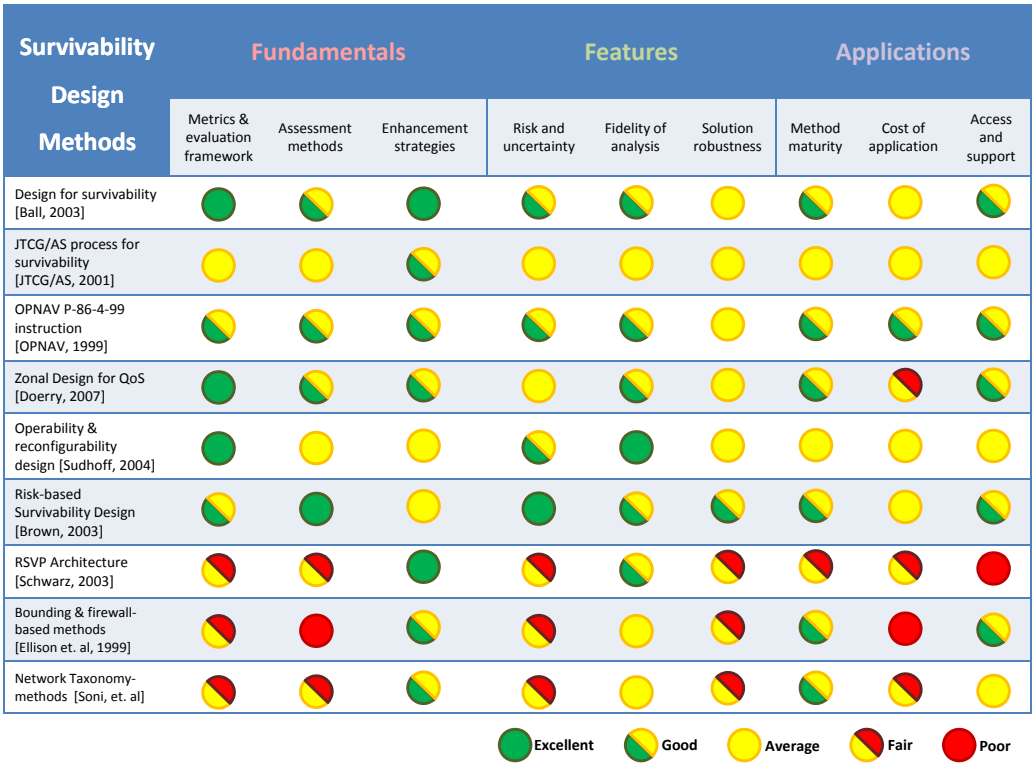


Figure 26: Evaluation of safety by-design methods

been qualitatively evaluated against nine criteria. The criteria were grouped into three categories, method fundamentals, features and applicability, and more information about the criteria development and selection can be found in Appendix B. Figure 26 presents the method evaluation, in the form of qualitative ratings. These methods effectively range from requirements and regulatory documents, to complete experimental approaches for assessing safety and the impact of possible enhancements.

Regarding method fundamentals, such as metrics and evaluation frameworks, assessment methods and recommendations for enhancement strategies, there is an obvious strength towards the latter. Each method carries their own unique sets of metrics for safety assessment and design, however these appear to be domain specific. Assessment methods are necessary for design iterations and testing, yet these mostly address safety through quantitative estimations, of risk, reliability and maintainability. Most methods point out the design improvements that must take place

for enhancing safety, however, these are present in the form of recommendations and seldom as steps within quantitative procedures of safety by-design methods.

Observation 2.1: Safety engineering methods range from certification and standards guides, to quantitative methods with steps on risk assessment and optimizing a design for safety. All methods offer suggestions on safety enhancement design strategies.

Figure 26 also describes the level at which risk and uncertainty are addressed, the fidelity of analysis for generating data, and whether methods investigate solution robustness. Most methods rely on historical information to perform probabilistic risk assessment, and fewer on the more expensive option for high fidelity modeling and analysis. Solution robustness is not always addressed from a design space exploration perspective, but it's implicitly present through capable technology selection that return system designs, which would be safe and survivable under several cases of adverse events.

Observation 2.2: SoA safety by-design methods mostly rely on probabilistic risk assessment techniques for testing and evaluation, rather than on more cost intense, higher fidelity modeling and analysis tools. Solution robustness is either addressed through design space exploration and reliability optimization algorithms, however more practical approaches depend on safety oriented technology infusion.

The last evaluation group explores method applicability, in terms of method maturity and readiness, cost of application, access and support. Policy-based methods, despite the fact that contain information with insights on safety improvement and evaluation, do not constitute a systematic procedure with design space exploration, or optimization routines that would return solutions for system configuration. The fidelity of analysis and modeling approaches used determines the cost of implementation. Access and support is a significant factor for its usability. Methods that are of high national or strategic interest, can be fully or partially proprietary, and

can sometimes be less attractive to use. Methods that are open for public use, are often effective in conceptual design, yet the lack of support or documentation can sometimes prove them inadequate.

Observation 2.3: SoA methods that are publicly available, tend to be high level, sometimes generic and less mature for a certain application. More systematic safety by-design methods with higher applicability and readiness, are application specific, often proprietary, and in many cases follow advanced modeling and simulation practices for evaluation, testing and design.

2.2 Survivability engineering

Recalling from Appendix A, system effectiveness is dependent on system availability, capability and dependability [97]. Dependability is a system property that integrates reliability, availability, safety, security, survivability, and maintainability [15]. If these "ilities" are not dynamically affected by time-dependent change, it is presumed that survivability effectively represents dependability in the effectiveness equation, and can be generally reformulated as:

$$SE = f[(Availability), (Survivability), (Capability)] \tag{3}$$

where other dependability factors (e.g. maintainability, safety, reliability) can be represented by the survivability term:

$$Survivability = g((Safety), (Reliability), (Maintainability)) \tag{4}$$

To further support this presumption, system availability is linked to mission logistics and dynamically depends on survivability. Capability is brought in as a design attribute, which represents the expected ability of the system to successfully operate and accomplish its mission. However, if a system does not survive in its operating environment, neither capability or availability is preserved. At that point, it is system

survivability that determines effectiveness and mission success based on the system's response to a threat [16]. Therefore, within the context of this research, system survivability is the primary focus as a means of concurrently maintaining availability and benefiting from capability, in a direction towards designing more effective systems.

2.2.1 Overview of system survivability

Historically, the concept of survivability was initiated by military operations [18], and has proliferated during the last fifty to sixty years in the form of military *combat survivability*. Its significance has been marked by the loss of approximately 5,000 aircraft to enemy fire in the Southeastern Asian Conflict (SEA) [18] in the years from 1963 to 1973. This milestone brought a new philosophy in military system design, where survivability has become a critical system characteristic, and has further evolved to a distinct design discipline.

Civilian systems are often exposed to hazardous conditions that could potentially lead to accidents. System safety promotes the understanding of accidents, through fault identification and monitoring of resulting system failures, the interactions with other changing environmental factors, as well as possible operator errors [17]. While system safety is concerned in mitigating the impact of threats and hazards, system survivability is not guaranteed solely through safety. Given that commercial systems must also withstand the impact of a hazardous environment and continue its mission while maintaining safe conditions for its crew and its passengers, system survivability is a crucial priority, in non-military systems as well.

System safety and survivability complement each other through a synergy of design solutions for hazard and failure mitigation, with the objective of maximizing survival of the system and its occupants in all environments [17]. This synergistic nature is underlined by technologies, initially developed for military systems, but are then often adopted to non-military applications (aircraft, ships, cars, networks). For

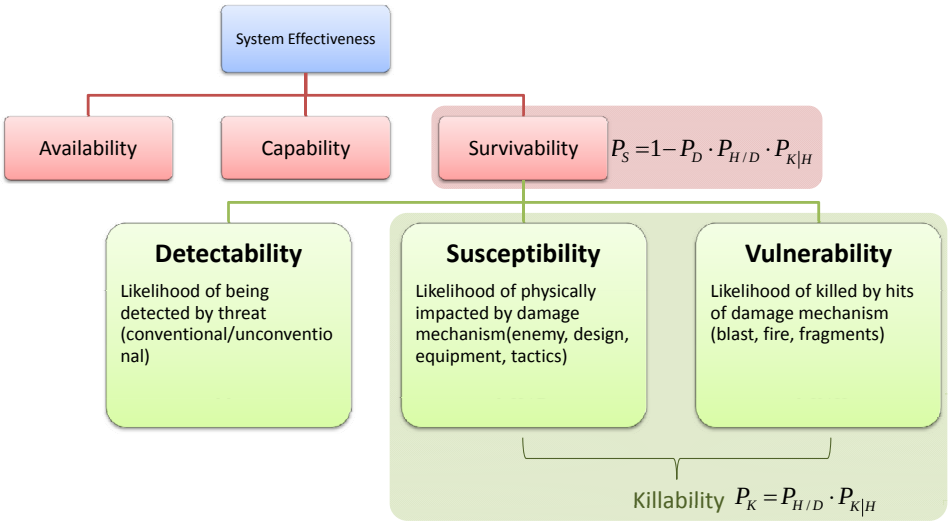


Figure 27: Measuring survivability [16]

instance, fuel system fire/explosion protection technologies, that have been developed for military aircraft, are now fitted into civilian airliners (following the loss of TWA 800) is an actual example of this common practice [17].

2.2.1.1 Traditional definition of survivability

Original definitions are relevant to military applications, the proliferation of survivability engineering in multiple scientific areas, however, has lead to a diverse ecosystem of theoretical frameworks, technologies and applications. The classic survivability formulation, as it has been applied by the military engineering community, is given though the following simple equation [16]:

$$P_S = 1 - P_K \tag{5}$$

where, P_S is the probability of survival and P_K is the killability or probability of not surviving the disturbance.

Depending on the type of the disturbance, if this happens to be an external attack, the equation becomes [16]:

$$P_S = 1 - (P_H \cdot P_{K/H}) \tag{6}$$

where, P_H is the probability of being detected (also known as susceptibility) and $P_{K/H}$ is the probability of not surviving the attack hit and getting killed, after being detected and attacked.

Susceptibility is the probability that the system accepts a direct attack hit or experiences secondary hit effects [16]. It is the system's inability to avoid disturbance, at least on one of its basic functions, by one or more threats during its mission [16]. System susceptibility is dependent upon three major factors: the threat, the system, and the mission. A threat is described by its characteristics and the effective impact on the system, which itself depends on its exposure to the threat by its observable parts. The mission indicates the physical operating environment, in which the threat becomes active. The importance of susceptibility relies on the fact that a threat can often be entirely avoided, making the system not vulnerable at all. From Equation 6, vulnerability is a conditional probability that depends on the outcome of a threat, while susceptibility is a probability that solely depends on whether the threat was experienced or avoided.

Vulnerability is defined as the conditional probability that the system is killed after it experiences a direct hit or secondary hit effects [16]. It is the system's inability to withstand the damage caused by a (often man-made) hostile environment, to its exposure and to its liability to serious damage or destruction when hit [16]. The more vulnerable a system is, the more likely it will be killed when attacked by multiple threats. Systems become vulnerable to threats, if they originally failed to avoid the threat. In complex systems, overall system vulnerability depends upon the subsystem vulnerability. However, this does not necessarily imply that a system with vulnerable components, will demonstrate increased vulnerability to threat, especially under the presence of unpredictable emergent behaviors in changing environmental conditions or threats [122].

The particular formulations of the survivability equation depends on the assumed

Figure 28: The Kill Chain [16]

sequence of events, after the system experiences a threat. In military systems, a *kill chain* is used to describe the chain of events, according to the system-threat encounter scenario [16]. Kill chains support probability calculations in system survivability assessment. For instance, according to the kill chain of Figure 28, the key conditional probabilities are defined and thus allow for the reformulation of Equation 5 as follows:

$$P_S = 1 - (P_H \cdot P_A \cdot P_{D/A} \cdot P_{L/D} \cdot P_{I/L} \cdot P_{H/I} \cdot P_{K/H}) \tag{7}$$

2.2.1.2 Survivability in science and engineering

Survivability has proliferated in several other scientific and engineering fields [191]. Survivability is considered as a design attribute in naval or merchant ship design [27], [173]. In civil engineering and architecture, infrastructure and large scale system survivability is improved against natural disasters (e.g. earthquakes, flooding, hurricanes) [19], [34]. Occupant protection in automotive/locomotive systems is another form of survivability, with focus on protecting human passengers [236]. Security and protection from malicious and hostile attacks against software (e.g databases), hardware (IT support, banking central systems), implicitly seeks to ensure the survival of physical devices, along with system functionality and operations [231]. In natural sciences, disciplines, such as biology [56], computer science [6], systems network theory [133], etc., apply survivability within their own context.

A generalized, inclusive definition for survivability is an open challenge for engineers and scientists. Most current definitions are specific to the application domain. But, given that the survivability concept is quite broad, with observed commonalities across disciplines and applications, it is presumed that a generalized, system

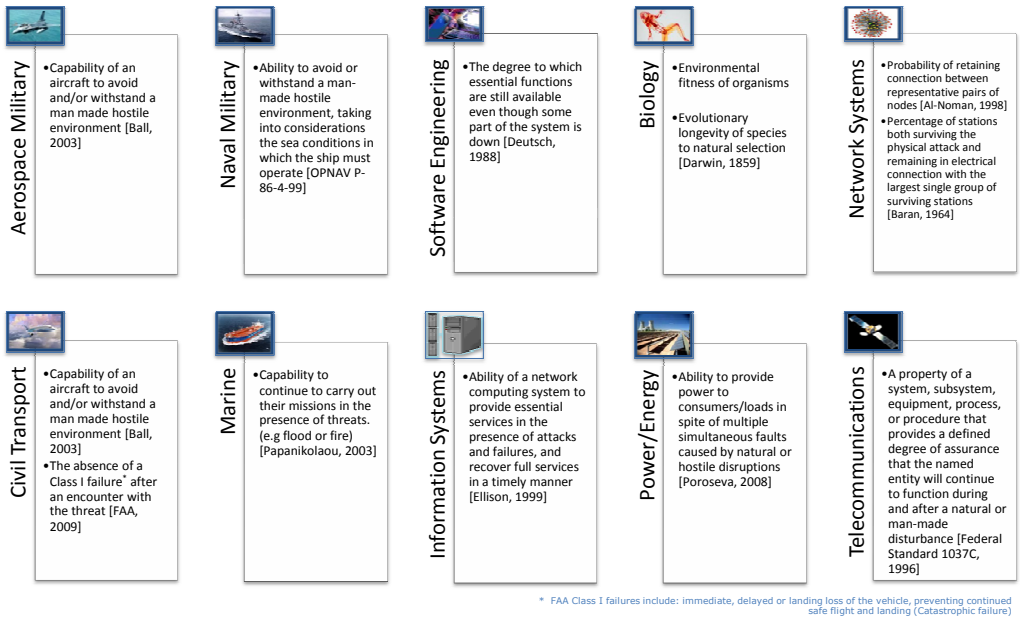


Figure 29: Survivability definitions for various engineering and scientific communities

independent and inclusive definition is feasible. A literature search across different engineering disciplines and scientific fields has been conducted, regarding definitions and application frameworks. Figure 29 contains a brief summary of definition finding, while for more information and details on how survivability is defined in each field, the reader is referred to Appendix C.

The literature survey has revealed strong similarities in keywords and concepts.

Observation 2.4: In the majority of disciplines, survivability is emphasizing the ability of a system to preserve itself and its mission under the occurrence of disturbances in a timely manner.

Moreover, there are three key characteristics of survivable systems [198]:

1. **Essential functions**: Survivable systems must be capable of performing a set of essential functions at all times. These functions are not necessarily linked to mission goals and objectives, but allow for "safety mode" operations. System survival however, could often depend on the system's mission success entirely.

Thus, a system can accomplish its mission successfully, when it can provide a service through producing an outcome, and delivering a value that satisfies the original system objectives.

2. **Attacks and failures**: Survivable systems must protect and maintain their essential functions, therefore their total health and their mission success, if any disturbances are experienced. A disturbance is a form of system interruption on essential functions and mission ability, and describes attacks, or faults and failures that could lead to accidents, or disasters. All systems have a natural ability to absorb disturbances, however, designing for robustness and resilience is one of the grand challenges in survivability engineering.

3. **Timely manner**: Survivable systems must perform their essential functions and respond to disturbances within certain time frames. Complex system behavior is highly dynamic, and this affects survivability. Thus value delivery is *time dependent*, especially considering that a disturbance may unexpectedly appear at some time point during the mission, and last for an unknown time period.

Similarities in survivable system characteristics support the prospect of introducing a generalized definition of survivability, independent of systems, platforms and disciplines. Based on the same three common observations for different types of engineering systems, Richards et al. [191] have defined survivability:

Survivability is the ability of a system to minimize the impact of a finite disturbance on value delivery, achieved through either:

- the satisfaction of a minimally acceptable level of value delivery during and after a finite disturbance or

- the reduction of the likelihood or magnitude of a disturbance.

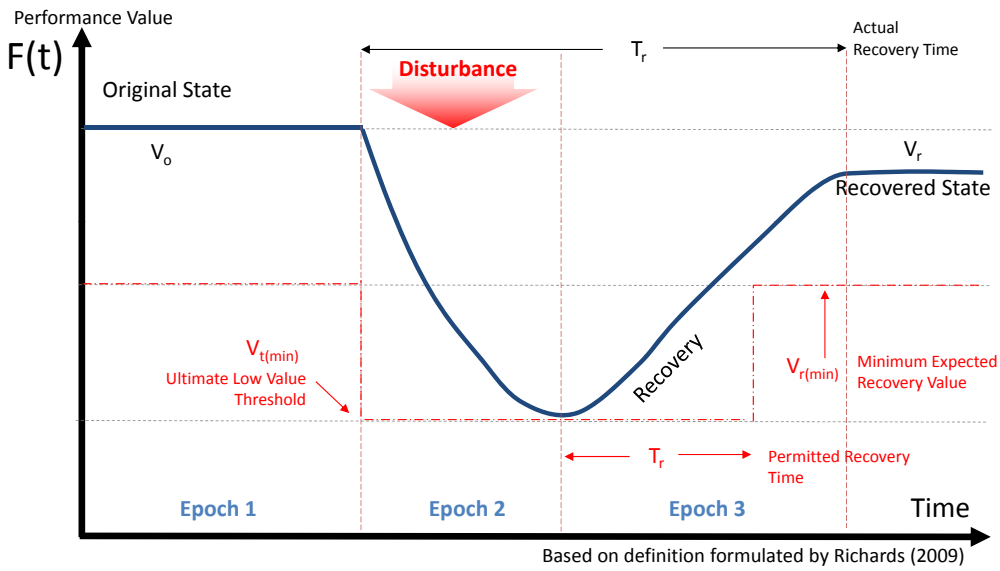


Figure 30: Towards a unified and global definition for survivability [198]

Figure 30 illustrates the typical behavior of a dynamic system that survives a disturbance [198]. Time is divided into *epochs*, namely time periods with a fixed attributes, such as static constraints, fixed design concepts, technology selections and properties [198]. Epoch 1 assumes normal environmental conditions, with the system being able to deliver a certain performance value V_0 at its original state. A disturbance suddenly occurs, resulting in system performance degradation with time and reaching a minimum, at the end of the second epoch. At the third epoch, the system is attempting to recover and reach its original value delivery state V_0, within a certain recovery time. The system does not always have to return to V_0 in order to survive, but it may be adequate if it restores to a performance value higher than the minimum expected $V_(r(min))$, no later than the permitted recovery time $T_(rp)$.

In conclusion, system survivability is seen as a concept, metric, design attribute. Despite the domain specific definitions and quantitative frameworks, the basic concept remains similar across disciplines. Survivability is highly dynamic in uncertain and changing environments. Overall ,a survivable system must be capable of continuously performing its mission and be safe enough in order to bring itself back into full

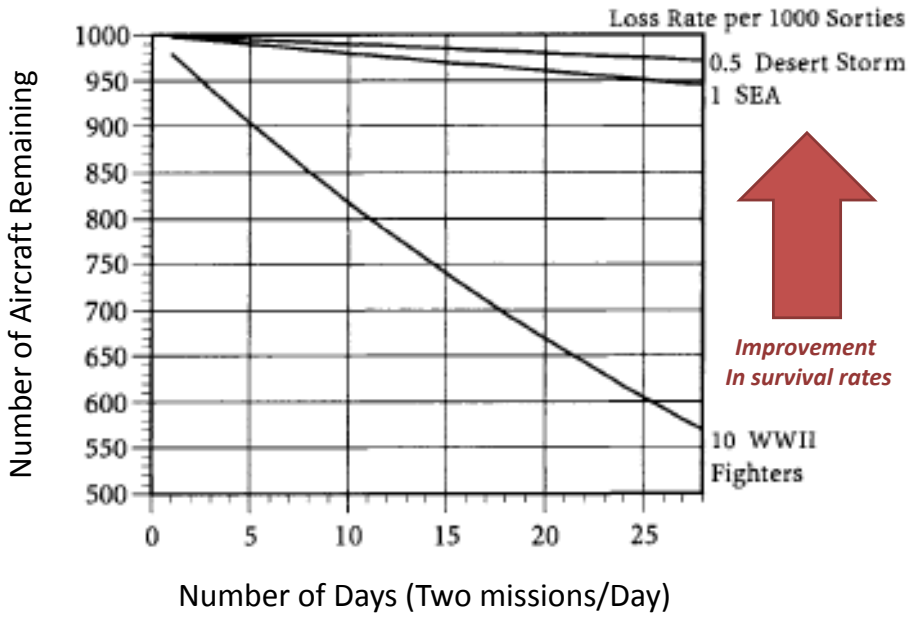


Figure 31: Fighter aircraft loss rates in historic campaigns [16]

recovery, within a recovery time T_r.

2.2.2 Applications of survivability-based design

Survivability-based design methods have been developed and originally applied for aerospace and naval military systems, since the 1950s. Figure 31 compares losses in fighter aircraft, for three historic campaigns, World War II, the Southeastern Asia conflict (SEA) and operation Desert Storm, and essentially illustrates the improvement in survivability, with loss rates becoming much lower for the most recent campaigns [16]. Over the past two decades, application of survivability-based design methods has expanded beyond military, aerospace or naval systems to include networks [170] (communication, transportation, power distribution, etc.), infrastructures [19], [34] and organizations.

The literature investigation has concentrated on survivability-based design methods for military systems, aircraft and naval ships, as well as complex networks. The most prominent ones are listed in the following:

1. Aircraft design for survivability by Robert Ball [16].

2. Methods by Joint Technical Coordinating Committee for Aircraft Survivability (JTCG/AS)[209].

3. Zonal design for naval survivability by Norbert Doerry.

4. Risk-based survivability design by Alan Brown.

5. Intelligent architectures for survivability and operability.

6. Survivable networks and IT systems.

2.2.2.1 Aircraft design for survivability

The Department of Defense (DoD), the Federal Aviation Administration (FAA) and other government agencies have published regulations and directives for advancing survivability and airworthiness. Driven by customer requirements and government regulations, survivability-based design for air vehicles is centered around viable, cost-effective technologies [150], aiming to reduce susceptibility and vulnerability [16]. Ball's method combines survivability assessment techniques with susceptibility and vulnerability reduction concepts [16].

Based on susceptibility and vulnerability assessment of baseline designs, the goal is to examine the impact of design enhancements on system survivability, along with associated costs for the upgrades. Cost-effectiveness analysis determines the benefits of survivability enhancing solutions, against overall mission effectiveness, as well as acquisition and operating costs [16]. If targets are not met, iterations on the design, and further assessments are necessary. An overview of Ball's methodology for selection of susceptibility and vulnerability reduction features is illustrated in Figure 32. The steps for survivability-based design are the following:

1. Mission threat encounter analysis.

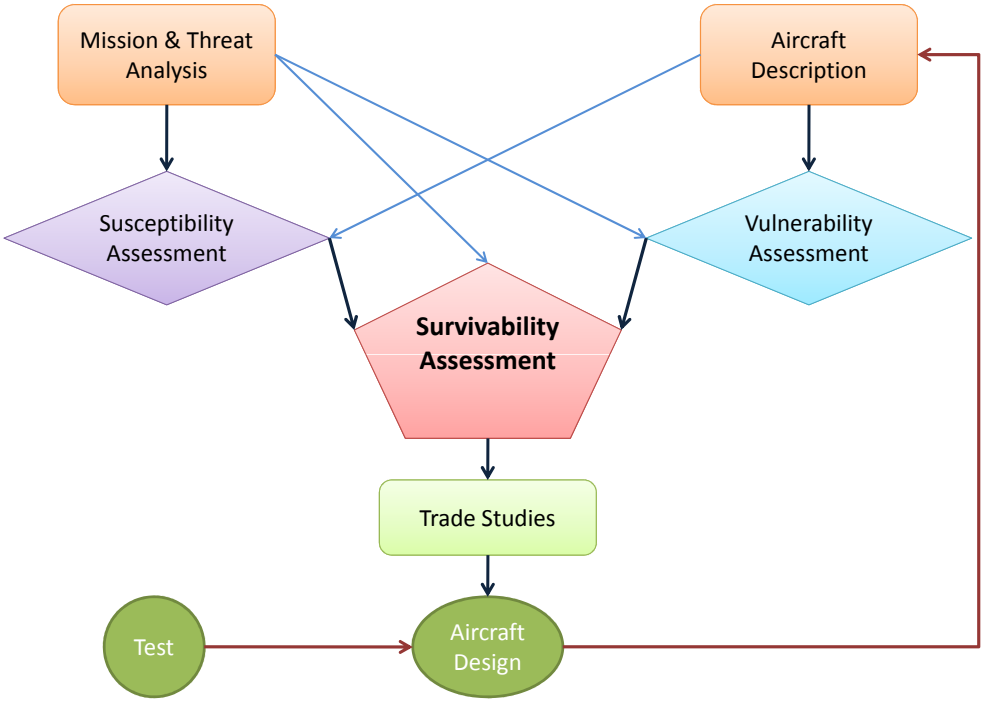


Figure 32: Ball's method for survivability based design [16]

2. Flight & mission critical functional analysis.

3. Failure and damage mode analysis.

4. Susceptibility analysis.

5. Vulnerability analysis.

6. Survivability analysis.

7. Survivability testing.

8. Survivability enhancement trade studies.

The first three steps are equivalent to a system and threat identification process. The next three analysis steps, are the basic modules of the complete survivability assessment for a given baseline design, if subjected to a given set of component fault or failure scenarios. Survivability testing for certification purposes, is based on hardware

Table 1: Mapping of engineering systems to failure types [16]

Susceptibility reduction	Vulnerability reduction
Threat warning	Component redundancy with separation
Noise jamming and deceiving	Component location
Signature reduction	Passive damage suppression
Expendable	Active damage suppression
Threat suppression	Component shielding
Weapons and tactics, flight performance	Component elimination
Crew training and proficiency	Component replacement

prototypes and is mandated by government agencies at the latter product development stages. For instance, live fire testing (also mandated by congress) is a realistic survivability and lethality testing for newly developed military aircraft. Other survivability aspects that need to be tested is the footprint of the vehicle, as well as signature management. Structural vulnerability is another feature of interest, indicating the ease of repair after damage, that allows for system recoverability.

Enhancement strategy selection (e.g. technology additions or architecture modifications), is based on survivability assessment, testing, and cost-effectiveness estimations. As an example, Table 1 lists six concepts that were implemented in the F/A-18 for susceptibility and vulnerability reduction. Figure 33 schematics illustrate how the concepts eventually made their way in the F/A-18 [16].

Typical options for reducing susceptibility include attrition management, ammunition increase, stealthiness improvement, addition of electronic equipment, while constantly updating the mission profile [16]. Accommodation, cooling and protection of electronic warfare equipment (threat warning, noise jamming and deceiving) must be considered as well. Signature reduction (such as radar signature or IR signature) is an inclusive susceptibility reduction strategy that extends beyond technology infusion to the overall design philosophy. However, conflicts or performance downgrades may arise due to technology or design incompatibilities, e.g. stealthy designs can lead to

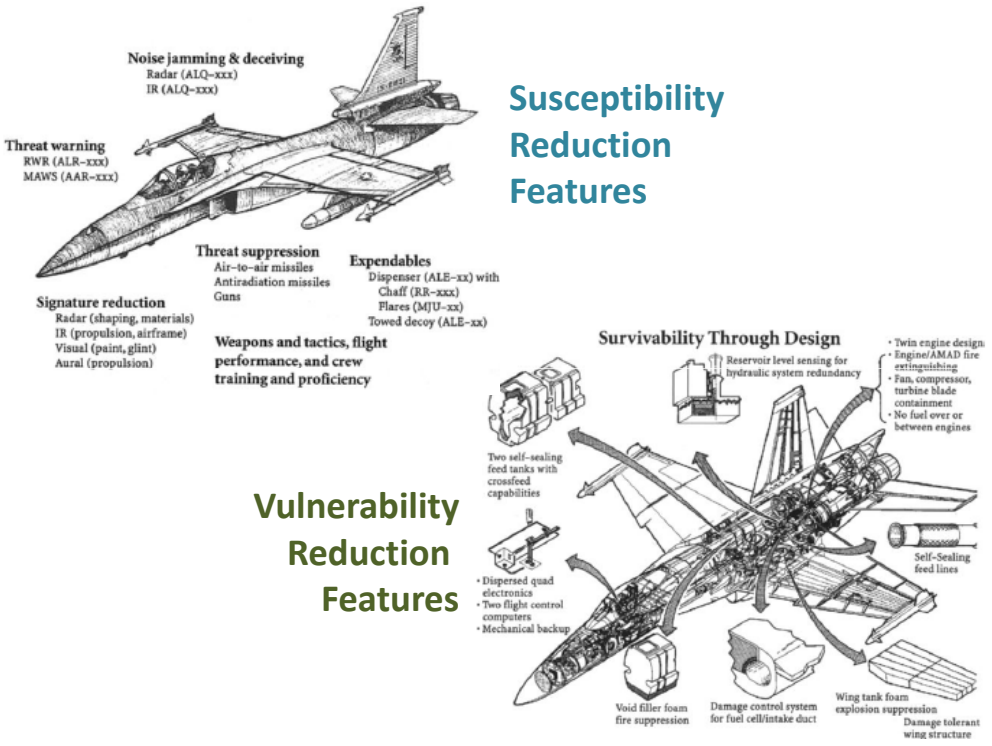


Figure 33: Susceptibility and vulnerability reduction features for the F/A-18 [16]

statically unstable aircraft [18]. For the successful implementation of these options, improved manufacturing procedures are necessary, contending with different materials, higher tolerances, complex shaping requirements, and suitable sensor placement optimization for minimum contribution to the system's signatures.

Vulnerability reduction techniques concentrate on four key requirements:

- Protect critical components (through redundancy and separation).
- Protect critical functions (lift, thrust, control).
- Improve system reconfigurability.
- Control damage propagation (maintain structural integrity and fire suppression).

The six basic concepts on the right side of Table 1 are options for supporting the four requirements in designing for low vulnerability. The major requirement however, is

that all occupants be protected, regardless of the damage or fault tolerance of the system.

Architecture-based design practices, such as *component redundancy*, allow for additional resources and capability, if the primary components become inoperable. *Separation* of components, or distribution on a physical architecture commands for more sophisticated and intelligent component allocation, given that certain locations and areas are more exposed to threats than others. Component elimination or replacement is targeting on ease of maintenance and supports intelligent resource allocation in real time. Active damage suppression relies on damage avoidance or control systems that the system hosts, while passive damage suppression is implemented through strategic architecture design and energy absorbing materials selection for improving crash survivability. One of the expected outcomes of low vulnerability is *graceful degradation*, which provides enough time for occupants to safely abandon the system.

2.2.2.2 The JTCG/AS process for survivability engineering

The Aerospace Systems Survivability Handbook Series was developed by the *Joint Technical Coordinating Committee for Aircraft Survivability* (JTCG/AS) to provide guidance to government and industry survivability managers, engineers and analysts involved in systems acquisition [209]. Recommendations for survivability-based design start from survivability requirements for a system, and evolve throughout the entire system acquisition process, while extending through the development, test, and evaluation of system prototype models.

The proposed design process is summarized by the following steps:

- Perform trade studies.
- Perform system and item analyses of the candidate design.
- Establish design criteria.

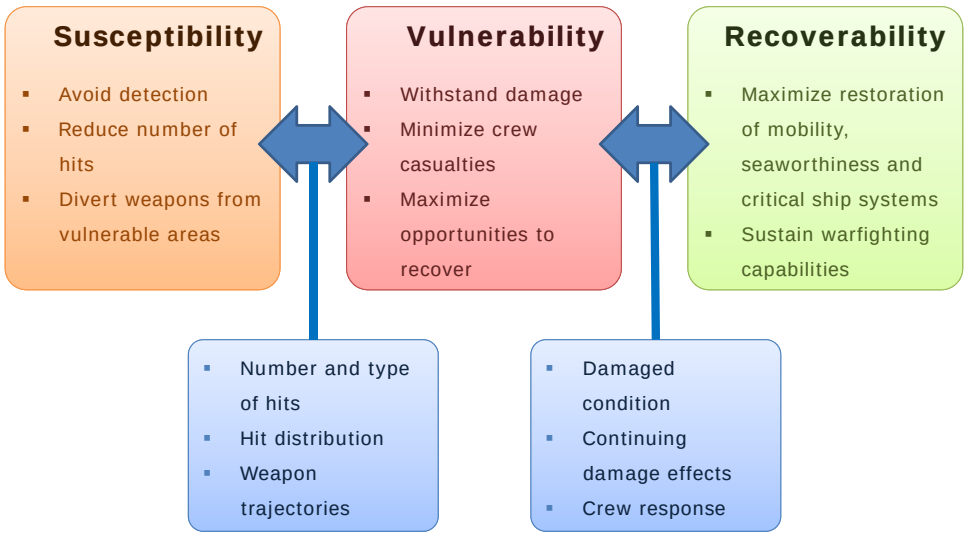


Figure 34: Survivability domain as defined by OPNAV P-86-4-99 instruction [245]

- Make detailed decisions that transform requirements, resources, and constraints into design.

Survivability enhancement trade studies return the relative contribution of a single enhancement to overall combat effectiveness, cost, and schedule. It is quite possible that an improvement through enhancement, is also combined to detriments in other response figures. Decision making on final enhancement must focus on a compromise that returns optimal system survivability in terms of total figures for combat effectiveness, cost, and schedule. This approach is based on traditional systems engineering practices for susceptibility and vulnerability enhancement, however, it may lack the required depth and insight that is required for this analysis in the conceptual design phase.

2.2.2.3 OPNAV P-86-4-99 instruction

Similarly to (JTCG/AS), there have been equivalent initiatives within the naval systems community that promote survivability as a design discipline. The U.S. Navy has a standard procedure for survivable ship design and survivability assessment, that is published through the *Survivability Design Handbook for Surface Ships* [245]. The

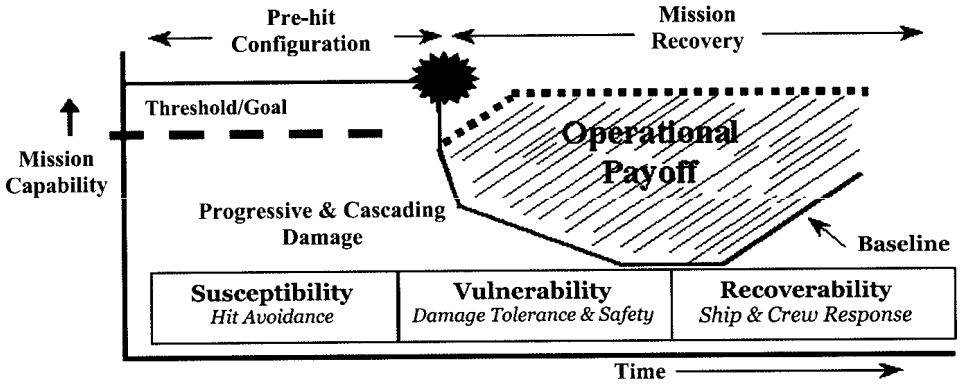


Figure 35: Elements of dynamic survivability [245]

OPNAV P-86-4-99 instruction [245] is the most prominent amongst naval engineers, providing definitions, metrics, and design processes for susceptibility/vulnerability reduction.

The Navy defines survivability as a probabilistic measure that depends on ship susceptibility, vulnerability and recoverability, as composed in Figure 34. From a dynamic perspective, the three survivability components can be described as in Figure 35, given that the system will degrade, but it will maintain its ability to recover.

The proposed design methodology relies on susceptibility and vulnerability reduction techniques, as revealed by Figure 36, which also describes the objectives of the process. The core of the method is the improvement of operational performance, however, life cycle cost issues are addressed, along with the identification of technical risks for the design procedure (design feasibility, producibility and supportability). In addition to susceptibility and vulnerability, there is special consideration of recoverability, mostly from the ship's dynamic stability aspect, as well as damage identification and repairability.

The survivability-based recommended procedure for total ship acquisition is illustrated in Figure 37. The first step of the process is the formulation of system requirements. It requires input from the Mission Needs Statement (MNS) for a new ship

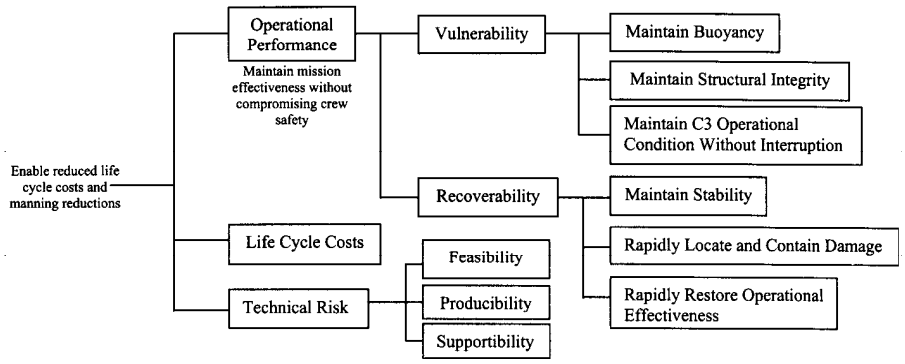


Figure 36: OPNAV Total Ship System Survivability Objectives and Procedure [245]

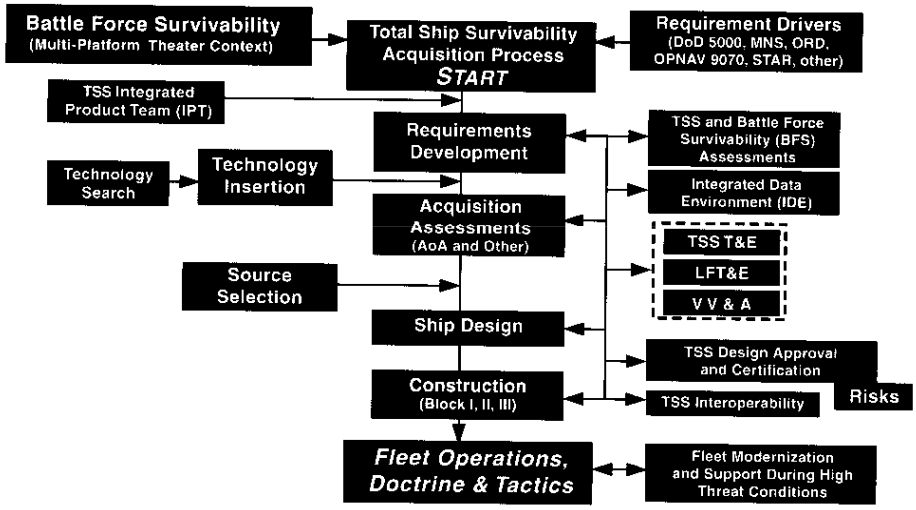


Figure 37: OPNAV Total Ship System Survivability Acquisition Process [245]

or naval system, which typically describes the desired operational system capability, along with SoA shortcomings, thus introducing the need for a new concept. The MNS then translates to the Operational Requirements Document (ORD), namely the formal requirements statement. It clearly outlines the expected capabilities, which must be transformed into technical requirements. Typically the technical requirements are driven by the survivability objectives, as shown in Figure 36.

The formulation of a baseline solution, is the input to the second step of the OPNAV process that suggest a series of assessments. These assessments address Total Ship (TSS) and Battle Force (BFS) Survivability, live fire testing (either virtually or

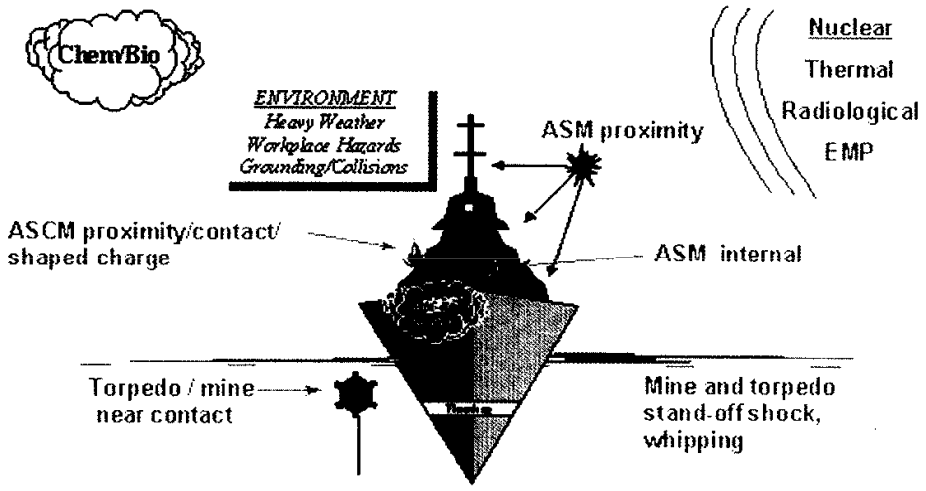


Figure 38: Threat environment for survivability assessment [245]

experimentally) and volumetric vulnerability assessment. Other testing sessions are necessary for survivability certification and approval. In conclusion, the TSS and BFS assessments investigate the total ship survivability, and discover potential gaps and shortcomings. Assessment results indicate the directions of improvement and allow for selection of survivability enhancement strategies. To conduct the assessments, sets of operational scenarios must be formulated, which reflect realistic events, such as torpedo or missile attacks, mine contacts or extreme natural environmental conditions, as shown in Figure 38.

There are several options for translating scenarios into practical, executable forms. The kill chain approach is one option, that applies for any type of military simulation. In naval applications, the kill chain additionally includes system recoverability, as presented in Figure 39, for a naval combatant mission scenario.

With a finalized list of design enhancements for survivability, the third step is to optimize system performance and perform tests and evaluations, in order to achieve the design requirements that have been set by the ORD. For susceptibility, the focus is on signature reduction through reducing the *Radar Cross Section*(RCS), heat and acoustic energy emission plus the ships magnetic signature. Susceptibility can also be

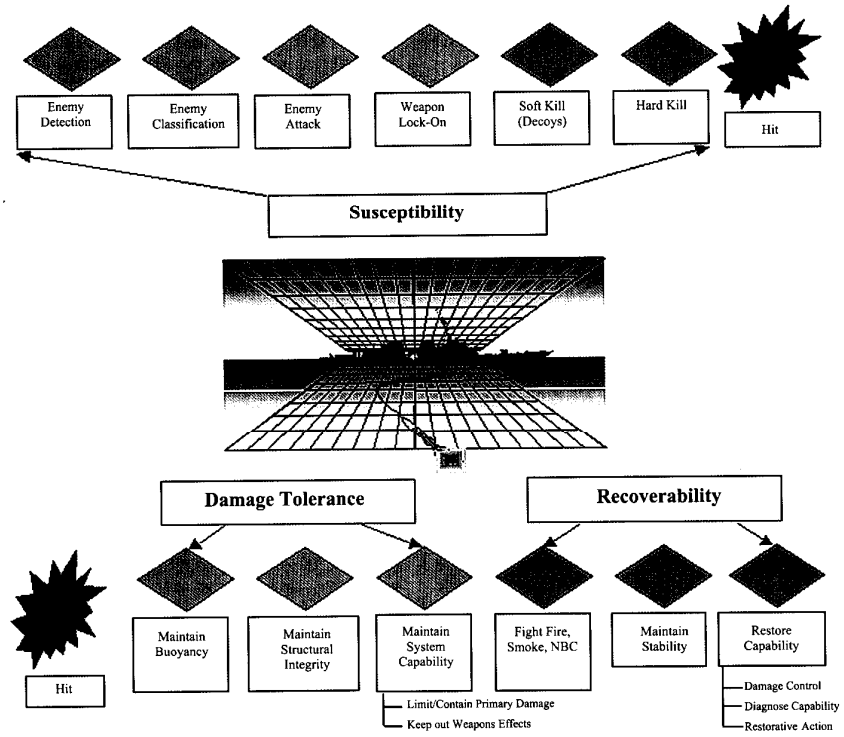


Figure 39: Kill chain for naval survivability assessment [245]

reduced through hull or mechanical/electrical system design, especially by improving weight distribution for better stability, maneuverability, component shielding, and overall situational awareness and readiness. Vulnerability reduction measures emphasize on maintaining ship flotation, stability, structural integrity and systems operability. Techniques for vulnerability reduction include subsystem redundancy, separation and intelligent distribution and co-location for vital ship operations.

2.2.2.4 Zonal design for naval survivability

Except for total survivability-based design approaches, it is quite possible to improve survivability by focusing on a particular subsystem, such as the power generation and distribution system of a naval ship. Zonal Ship design is a design philosophy for more survivable architectures, that brings focus on power system survivability [180], by monitoring the quality and continuity of service [64]. Quality of Service (QoS) [65] is a metric of how reliable a distributed system provides its value to the

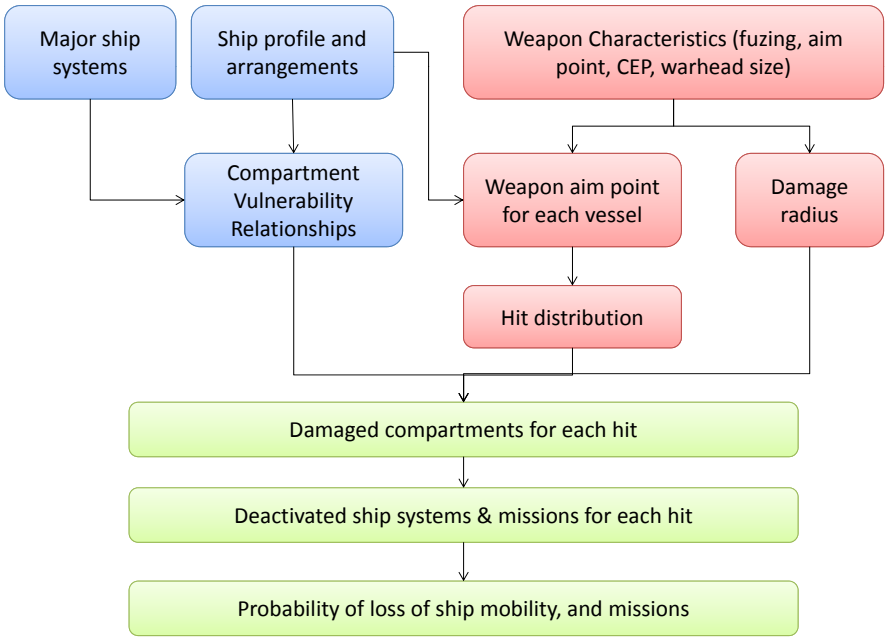


Figure 40: Volumetric Integrated Vulnerability Assessment (VIVA) [65]

end user and calculated as a Mean Time Between Service Interruption (MTBSI) as viewed from the loads. It is taking into account equipment failures, however it does not consider survivability events such as battle damage, collisions, fires, or flooding [65]. The ultimate goal is to maximize the *Quality of Service* (QoS).

Zonal design is applied at early conceptual design and feasibility studies [64]. With a concept of operations and baseline solution for the distributed systems architecture as a starting point, mission critical subsystems and component can be and the identified and allocated into zones. A key decision point is the identification of the zone boundaries. The boundaries of the zones must allow for zones that are large enough, such that any damage does not span more than two adjacent zones, yet, their size must allow for an adequate zone number, which ensures sufficient mission capability and survival, after the loss of any two adjacent zones [64]. Zonal design falls under a generalized design philosophy that calls for distributed system architectures, with subsystems that are not entirely independent, but interrelated to certain level [65].

With a given zonal configuration of the baseline distributed architecture, the analysis of the ship model for QoS estimations and survivability assessment, is performed through a computational ship synthesis tool, that reflects the selected component allocation in zones. QoS and survivability analysis depends on preselected threat scenarios, and evaluations are primarily driven by the power system architecture, subsystem reliability and system operations. To complete this step, the *Total Ship Survivability Assessment* (TSSA) method [245] has been chosen for the assessment. In support of the TSSA, the *Volumetric Integrated Vulnerability Assessment* (VIVA) [65], predicts the modes and rates of damage propagation through the architecture, as explained in Figure 40. Furthermore, VIVA returns the affected systems, within a given volume of space of the ship architecture.

The final stages of zonal design utilize the outcomes of TSSA and VIVA for QoS and survivability analysis, which will aid in determining the directions of improvement for better addressing the survivability requirements at the lowest acquisition and operating costs. Cost and performance drivers can be applied and in conjunction with design space exploration techniques, in order to concurrently optimize (e.g. Genetic algorithms, Monte Carlo methods, or gradient-based methods) for QoS, survivability and cost. To optimize the architecture, zonal design relies on two strategies, spatial redundancy and source-load alignment. Assuming damage control prevents damage propagation outside the damaged zones, spatial redundancy allows for the main systems to maintain operations, under the support of distributed subsystems [65]. Regarding source-load alignment, electrical system generation capacity is matched to load capacity within each zone. The strategy provides a level of autonomy for each zone, thus not always requiring zones to interconnect for power exchange. Survivability is enhanced, but this is not always the case for QoS, thus interconnections among zones is still permitted.

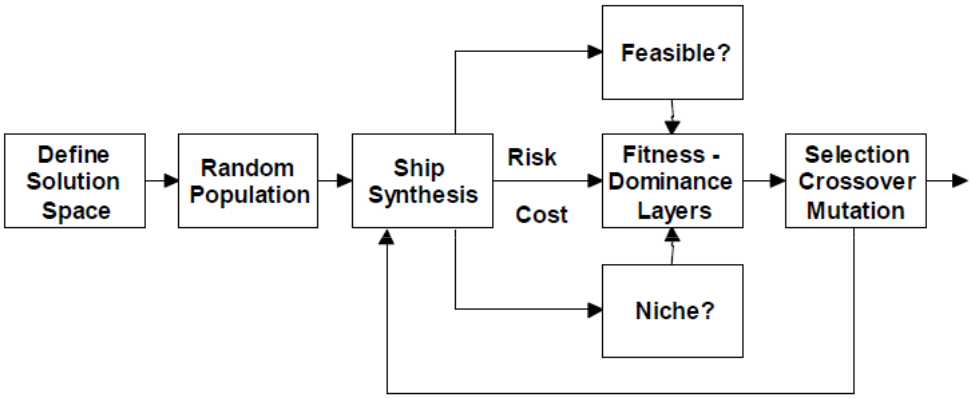


Figure 41: Risk-based ship design optimization procedure [33]

2.2.2.5 Risk-based survivability design

The Multi-objective Ship Design Optimization technique is a risk-based survivability design method, that has been demonstrated by Dr. Alan Brown, for merchant and passenger transport ships [32]. Influenced by the recommendations of the International Maritime Organization (IMO) and the SAFER-EURORO [204] initiative for merchant and ferry ships, the method aims to improve ship safety and survivability through a multi-objective function investigation of alternative solutions, against a given set of pre-generated scenarios. The objectives include functions for cost, effectiveness and risk. Design space exploration and risk optimization [26] is performed through risk-based decision making [31], e.g. with the Multiple-Objective Genetic Optimization (MOGO) algorithm that is presented in Figure 41 [32].

Probabilistic calculations are supported by two risk-based approaches, the risk objective attribute approach, or the uncertainty-based approach. With the first approach, risk is quantified as a single objective attribute, the Overall Measure of Risk (OMOR), representing the probability of failure associated with discrete failure events in system performance, cost or design inconsistencies and technology maturity [31]. With the second approach, risk is quantified through probability distribution functions for objective attributes (cost, performance), and is calculated by explicitly

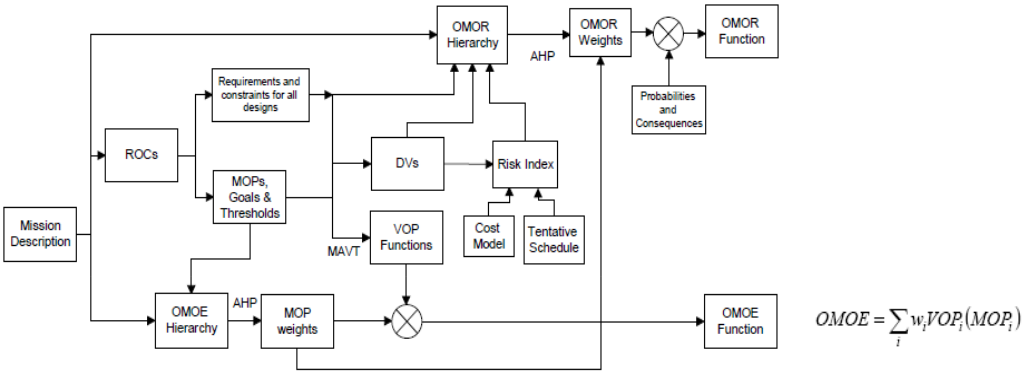


Figure 42: OMOE development process [33]

introducing uncertainty (inherent, statistical, modeling, technology, human) in the ship synthesis (modeling and analysis) process. The process for OMOR and OMOE calculation is shown in Figure 42.

Inspired by principles of axiomatic design, the suggested design process can be imagined as a sequential mapping between four domains: the mission or customer domain, the functional domain, the physical domain and the process domain [227]. It is concluded that uncertainty analysis is best applied in post-exploration design optimization, after specific cost and performance goals and thresholds have been set, to maximize the probability of achieving these goals [31].

2.2.2.6 Intelligent architectures for survivability and operability

The problem of survivability-based design for large scale systems, is alternatively approached from a system intelligence and control standpoint. This is a SoA approach, when systems need to be reconfigured and retrofitted with intelligent system technologies at the latter design stages. Design for intelligence and reconfigurability should be implemented concurrently to design for performance, mission effectiveness and affordability at the early conceptual design stages [193]. Under this philosophy, survivability relies on reconfigurable architectures and intelligent controls. Along these lines, Sudhoff's approach calls for optimization for naval power system operability

[225]. Another effort is the Reduced Ship's Crew by Virtual Presence (RSVP) initiative, the survivability problem is approached from a practical controls, health and status monitoring perspective [210].

Sudhoff's operability-based method, concentrates on the power generation and distribution system of a naval combatant. According to the method, operability improvements depend on enabling technologies that support reconfigurability and performance stability [225]. Systems engineering and architecting is a key enabler as well, subsystem integration for instance, as the next generation of naval shipboard power and propulsion systems will feature an electric drive-based propulsion system, which is fully integrated with a power electronics-based zonal distribution system.

Regarding performance, the immediate benefits include the increased efficiency at low speeds (through the use of an electric drive), an increased amount of electric power for pulsed power applications, and a high degree of robustness. Dynamic stability of both the AC and DC system portions must be further investigated [87], due to the large number of high-bandwidth constant power loads [226]. Analysis and testing is based on a layered computational total system model, in which each subsystem is represented through a separate layer [225]. To support decisions for architecture and technology selection, the method estimates baseline survivability, through numerical estimation of system availability for a given mission scenario.

In a more practical exercise, the Office of Naval Research (ONR) commissioned the RSVP Advanced Technology Demonstration (ATD) to develop a proof-of concept system [209]. The basic hypothesis implies that reconfigurable architectures with increased intelligence and automation, will enhance survivability. The goal of the RSVP ATD is to demonstrate the feasibility of a system that supports the hypothesis. Figure 43 describes the prototype architecture, that is composed of sensor units, Access Points (AP), System Health Monitoring (SHM), a Local Area Network (LAN) for the entire ship, and a watchstation.

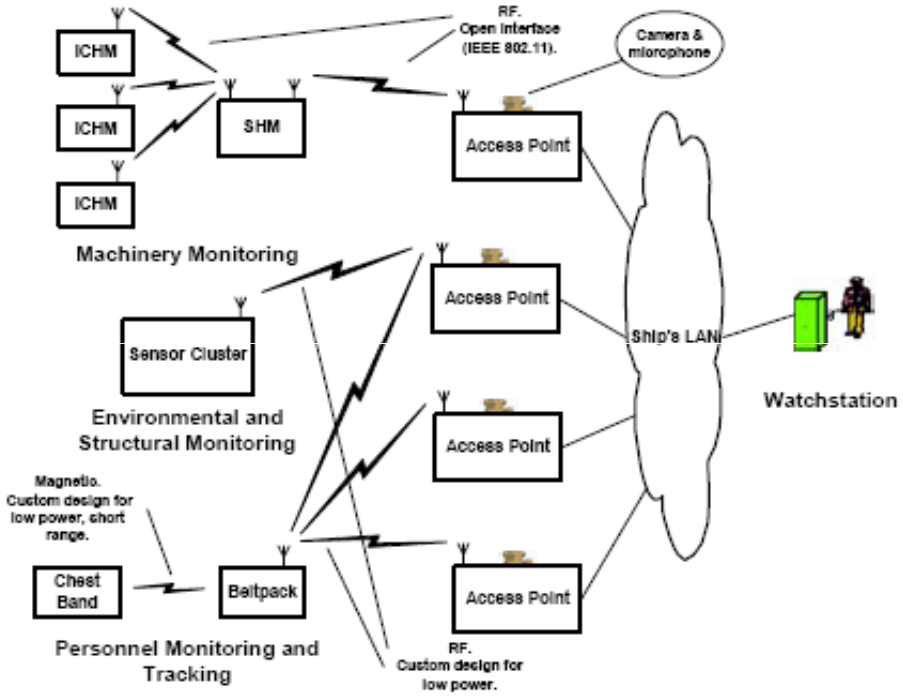


Figure 43: RSVP Architecture [209]

To reduce installation and maintenance costs, sensors are part of a large network, supported by wireless technologies. To further minimize costs, and improve reliability, efficiency and stability, Micro Electromechanical System (MEMS) sensors have been selected. More conventional sensors form the environmental sensor clusters, mounted on certain ship locations, and are tuned to monitor temperature, smoke, ionization, humidity, air pressure, flooding, oxygen, carbon monoxide levels, and acoustic transients [209]. Structural sensor clusters are mounted on beams and hull locations to monitor the ship's structural status, while personnel status monitors are devices worn by system occupants, to monitor crew member health status. Watchstations are the interface with the ship's operators.

2.2.2.7 Information technology (IT) systems and communication networks

Large scale complex architectures often include IT systems and networks of various size or configuration. IT systems can be either small or large, bounded or unbounded.

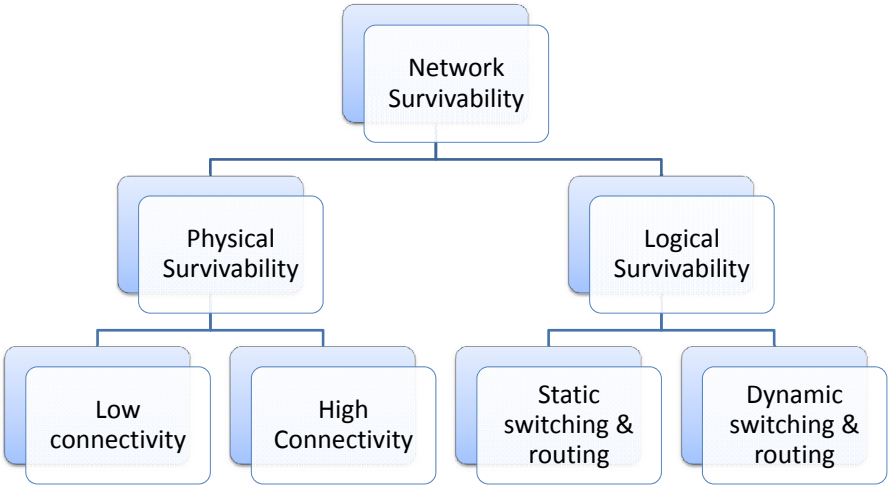


Figure 44: Network Survivability Taxonomy [219]

Most network-based IT systems are bounded (finite dimensions and specific location), however, such classification is not entirely accurate. For instance, the World Wide Web (the Internet) is an enormous, theoretically bounded IT system, yet what it really represents is an almost indefinite large scale network of systems.

From the perspective of security, and furthermore safety and survivability, size may not be as important as boundary allocation [72]. Risks are much higher for unbounded networks, as any individual node can be compromised, but all network essential services must still survive. Survivability-based design approaches for large scale networks aim to improve survivability through two different levels, the physical or the logical level, as visualized in Figure 44. System connectivity is what determines physical survivability, while switching and routing strategies affect logical survivability.

Assessment and enhancement approaches are highly based on heuristics for cases of low connectivity and static switching, with most SoA models address only single node failures. Work in the area of dynamic switching, is also limited with only a few optimization models developed so far [219]. Cutting plane heuristics is an alternative approach to networks of high connectivity [219]. Graph theoretical approaches are

the standard for network modeling, in support of network survivability analysis.

Survivability assessment or design methods for networks are dependent on the network configuration. In order to adjust to the network application, the concept of survivability reasoning frameworks has been introduced [74]. Understanding that environmental conditions can be dramatically different across different missions, reasoning frameworks take this variating factors into account, through incorporating such information in a collection of frameworks. For instance, an initial collection of reasoning frameworks is created, through classification of enemy tactics and environmental patterns into groups, based on the general scenarios to which they respond [74].

Classification through reasoning frameworks can be used as a prediction tool that could effectively narrow down the number of critical scenarios for survivability-based design. Moreover, it allows for predicting the likelihood of system disturbances, based on how context changes affect system modes of operation. A reasoning framework is associated with a set of general scenarios, where each scenario is comprised of six parts [74]:

1. **Disturbance**: Condition that needs to be considered when it affects a system.

2. **Source of the stimulus**: Entity that generated the disturbance.

3. **Environment**: Conditions and context under which the disturbance occurs. It can dictate the disturbance sources that can potentially threaten the mission. Disturbance sources (also "attackers") can be classified according to their resources (funds, personnel, and the skill levels), timing(very-near-term objectives, long term wait for opportunity), tools(sophistication level), risk aversion, system access, objectives (political, financial, criminal, military, personal).

4. **System response**: the activity undertaken after the arrival of the stimulus

5. **Response measure**: the attribute-specific constraint that must be satisfied by the response.

Regardless of recent approaches in for network security risk mitigation, most efforts concentrate on a narrow, security-based view of defense against computer intrusions [72]. Most remedies rely almost exclusively on system hardening (e.g., using firewall technology) for hacks or malicious attack prevention. Susceptibility measures, such as intrusion detectability and situational awareness, are mostly post-design additions. Networks are designed with performance and functionality in mind, rather than robustness and recoverability [72]. Survivability enhancing solutions assume a static network behavior, thus ignoring dynamic environment changes, or graceful system degradation [73]. Last, bounded-system thinking (e.g. firewalled sub-networks) within unbounded domains, effectively a logically bounded system within a physically unbounded one, could result to solutions that may be flawed from a survivability perspective. [72]. Work by Ellison et al., brings focus onto four network survivability aspects: resistance, recognition, recovery, and system adaptation and evolution.

2.2.3 Evaluation of SoA in survivability-based design

The methods and techniques for survivability-based design that were discussed earlier, are summarized in Figure 45, according to the most established applications. However, each method does focus on a particular aspect of the survivability problem. Some of these methods focus on certification checks for mandated minimum survivability requirements. Others bring emphasis on the accuracy and fidelity of the modeling and simulation analysis tools. Survivability assessment is a key enabler that is necessary for decision making on survivability enhancements. Most of them however, address the survivability design problem through assessment against certain threat classes, along with recommendations on design or technology-based solutions for enhancing safety and survivability.

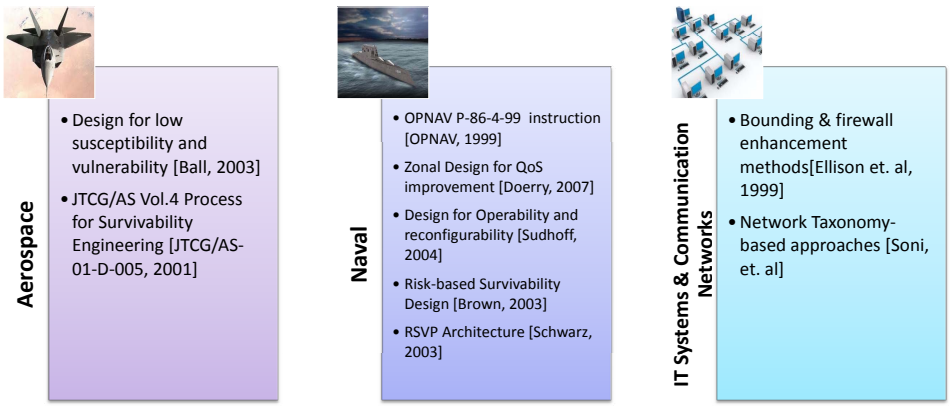


Figure 45: Summary of SoA in Survivability-based design

For the purpose of performing a comparative qualitative evaluation of SoA survivability design methods, the criteria that have been used for safety design method evaluation are applicable, and more information about their selection is found in Appendix B. The evaluation criteria have been grouped under three main categories (method fundamentals, features, and applicability) and the results of this task are presented in Figure 46.

A first look at the comparative evaluation table, it does appear that survivability-based design methods have been evolving non-uniformly across different disciplines and applications. It becomes obvious that military engineering applications, namely aerospace and naval possess the lead in terms of method theoretical development, effectiveness and applicability. Robert Ball's method is distinguished due to its rigorous, complete and thorough theoretical approach, yet it still maintains a proper level of generality to remain platform and application independent.

Observation 2.5: Survivability-based design methods follow the same basic process steps, however they do depend on the particular application. Robert Ball's method is an inclusive, rigorous approach that could serve as a basis for method development for any other engineering application.

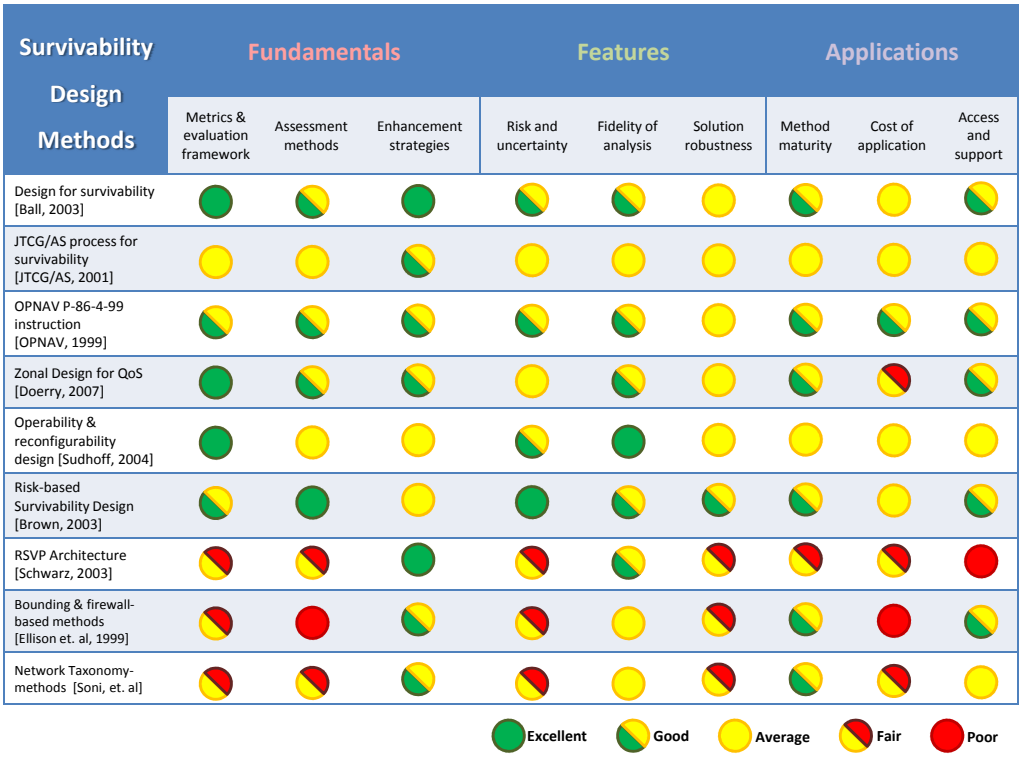


Figure 46: Evaluation of survivability-based design methods

It becomes apparent that survivability assessment techniques are absolutely necessary for evaluating of system survivability against certain tests, as well as for determining the direction of improvement for survivability enhancements. Formulation of the required experiments, relies on the aspects of survivability to be tested, namely susceptibility, vulnerability and recoverability. Most assessment methods focus on vulnerability, and either make use of historical data, or employ computational modeling and simulation. Recoverability is often measurable through performance data. Susceptibility analysis requires deeper mission understanding and further investigation regarding the impact of technologies, responsible for system situational awareness, threat detection and avoidance capabilities.

Observation 2.6: Survivability assessment is necessary for estimating the impact of technologies and design enhancements. Most approaches focus on vulnerability analysis, while susceptibility analysis usually requires different analysis and evaluation

frameworks.

Survivability is generally defined as the probability of survival, thus assessment and design methods are probabilistic. For more accurate survivability calculations, a large number of experiments, or number of runs is required, and depending on the application, there may be additional requirements for higher fidelity of the modeling and simulation environment.

Observation 2.7: Survivability-based design methods are probabilistic. Large numbers of experimental cases are required for better probability estimations. Selection of modeling tools must take into account the benefits to estimation accuracy against the cost of use.

Solution robustness is a measure of how well prepared the system is by its design, to respond to known, or less known external threats or environmental changes. To ensure system robustness, methods should provide techniques for system survivability testing under scenarios with expected threats, as well as some unexpected ones. Mission profiles can be the source of typically expected threats and operating conditions, but further research is required to formulate possible unexpected conditions. In the SoA, some techniques mention the above need, but other take a step further, by discussing scenario development techniques or how survivability testing should be made. For instance, power system design for survivability by Sudhoff [175], and Doerry [64] have more in common to robust design techniques. Others do underline the importance of robust design, yet further research for complete implementation is required.

Observation 2.8: As a consequence of operational uncertainty, robust design is a vital component of survivability-based design. To improve solution robustness, one must invest on modeling and simulation tools of higher fidelity, and on an extended

mission scenario set that includes more that the expected system threats and disturbances.

Method maturity reflects method applicability for a real life application. Ball's method [16] and the Navy's OPNAV P-86-4-99 [245] are mature methods, yet not immediately applicable to different systems, without prior adjustments to details. Method applicability usually depends on the system and the level of complexity of real world practical problems. Less general and structured approaches, rely on more particular issues around survivability design, especially on technologies and survivability enhancement solutions for components and subsystems. Cost of method implementation depends on method maturity and effectiveness. Theoretical and higher level approaches are more affordable, and are more suitable for conceptual design. More system and technology dedicated approaches are more expensive to apply, and in many cases less accessible or restricted. The latter refers to access and support, where methodologically mature approaches are open to implement, where technology-based, and survivability enhancing approaches that are dedicated to particular system types are more restricted and proprietary to non-affiliated entities.

Observation 2.9: Generalized approaches for aerospace and naval applications are methodologically mature. All necessary steps and processes are clearly outlined, yet they are not application specific or ready. Technology-based approaches mostly focus on survivability enhancements, thus less mature as complete methods. Cost of method applicability depends on system requirements and complexity. Last, more theoretical, generic and inclusive approaches are less restricted than more specialized and dedicated, technology-based ones.

2.3 Resilience engineering

Resilience engineering is an emerging discipline, that can be viewed as an evolution to traditional safety and survivability engineering practices. It brings a new perspective in understanding and analyzing system uncertainty, risk, and furthermore assessing safety and survivability. It has been established under a set of premises, which stem from limitations in understanding of how risk and uncertainty affect safety, or how system complexity may lead to accidents. Additional issues about complex system interactions in large scale operating environments contribute to overall uncertainty and nonlinear, dynamic system behavior. Hollnagel has summarized the basic premises of resilience engineering, in the following statements [109]:

1. Performance conditions are always underspecified.

2. Adverse events can be attributed to an unexpected combination of normal performance variability.

3. Safety management cannot be based on hindsight nor solely rely on error tabulation and failure probability calculations

These statements reflect limitations in current safety engineering practice. They are the fundamental directions, which resilience engineering has been addressing as continuously evolving, and emerging discipline.

2.3.1 Overview of system resilience

System resilience is not currently described by a unique and standard definition [146]. There are several definitions that are specific to a discipline or to an application. However, there must be common attributes in resilient systems of any application. In order to understand the basic characteristics of resilient systems, an extensive literature survey has been conducted.

Figure 47: The three basic functions of a resilient system

A *resilient system* can adjust its functioning prior to or following changes and disturbances so that it can go on working even after a major mishap or in the presence of continuous stress, mainly by being able to be proactive on safety [111]. The ability to be proactive is emphasizing the reduction in system susceptibility, by either preventing unwanted events and outcomes or eliminating hazards in the operating environment. Traditional safety, however is essentially reactive or passive and is addressing the need for vulnerability reduction, through withstanding outcomes of unwanted events, or reducing the adverse consequences of unwanted outcomes. In more practical approach, Hollnagel [109] has provided a template of the fundamental functionality that resilient systems must possess, that is also visually described in Figure 47:

1. **Anticipate** disturbances. That includes potential threats, various disruptions and any other destabilizing conditions. Implementing this function relies on

Figure 48: Scientific and engineering fields of resilience application

what model is selected to predict the future and under what tolerance for risk.

2. **Monitor** performance. Except for mission performance and system health monitoring, a resilient system must also be able to monitor risks and threats and continuously revise its own model of risk identification. This will allow for revealing of non-profound transient effects, that even though are not permanent, they can still contribute to failures and accidents.

3. **Respond** to threats. This function implies an intrinsic readiness, along with an inherent flexibility and adaptability in response to regular, irregular or unexpected, and unexampled events.

While resilience has been originally discussed around socio-ecological systems, equivalent forms of system resilience have appeared for other disciplines and applications [146]. Figure 48 lists most applications of resilience that have been recently

introduced, based on extensive literature search. Most applications are related to systems engineering, environmental and civil applications for instance, such as infrastructures, cities and communities, with resilience defined against disasters, earthquakes, major climate or other environmental changes [35]. In non-engineering applications, there is economic and financial resilience of an organization, and industrial or organizational resilience on a higher level. Resilience of networks, is an application that can refer to any system that is part of a networked structure. Human behavior and interactions form another application, under psychological resilience [189]. More insight on resilience, from the perspective of different applications, is provided through the following sections.

2.3.1.1 Ecological, environmental and civil systems

Holling's definition [106] associates resilience to the ability of a system to absorb a disturbance and maintain all its internal connections and functionality. Although some ecologists [178] consider resilience to be a measure of how fast a system returns to an equilibrium state after a disturbance (return time), Holling defined it as a measure of how far the system could be perturbed without shifting to a different regime (deviation tolerance). The return time, is now known as "engineering resilience", whereas the tolerance based definition refers to "ecological resilience", according to Holling's 1996 revision [107].

In environmental engineering, where optimal resource management is a necessity, resilience is defined as "the capacity to adapt existing resources and skills to new situations and operating conditions" [46]. Alternatively, Tielley et al., bring the aspect of flexibility and adaptivity, by explaining resilience as "both the inherent strength and ability to be flexible and adaptable after environmental shocks and disruptive events" [234]. Fiksel links resilience to sustainability, or describing it as "the essence of sustainability, or the ability to resist disorder" [83]. For engineering applications

where the infrastructure is viewed as an interaction with the local community, (local) resilience describes the ability of a community to withstand an extreme natural event without suffering devastating losses, damage, diminished productivity, or quality of life and without a large amount of assistance from outside the community" [159]. Community resilience may become specific to particular types of disasters, such as earthquakes (seismic resilience), water flooding, hurricanes and extreme temperature conditions.

2.3.1.2 Social systems

Community resilience refers to the reaction of an infrastructure to a natural disaster, in conjunction with a local community. If the disaster is extended to include any type of disturbance, with any possible impact beyond a local community, then this definition is generalized for social resilience. The latter is defined as the ability of groups or communities to cope with external stresses and disturbances as a result of social, political, and environmental change [4]. The 9/11 event was an intelligent, non-natural and intentionally caused disaster, that its consequences extended through-out an entire nation, and had furthermore created an impact on the rest of the world, thus social resilience within an entire country had been challenged.

2.3.1.3 Organizations

When systems are characterized by a composite, detailed, and highly interrelated structure, resilience is referred to as organizational resilience. It is the ability of a system to withstand stresses of "environmental loading" and a fundamental quality found in individuals, groups, organizations, and systems as a whole [113]. While the expected resilient behavior is similar, organizational resilience usually refers to systems that possess a known internal structure, either hierarchical or centralized.

2.3.1.4 Economic and financial systems

To further support the assertion that the concept of resilience would apply on any kind of system, in the case when disturbances are of economic nature, organizations may feature internal mechanisms that make them insensitive to the disturbance and also give the opportunity to adapt and recover. In other words, economic resilience is the inherent ability and adaptive response that enables firms and regions to avoid maximum potential losses [197]. Rose [196] introduced two types of economic resilience, that is static and dynamic resilience. Static economic resilience is the ability of an entity or system to maintain function when shocked [196]. On the other hand, dynamic economic resilience is the speed at which an entity or system recovers from a severe shock to achieve a desired state. In other words, static economic resilience is an instantaneous measure of the performance of an entity or system relative to a non-resilient or fragile performance, whereas dynamic resilience is harder to assess, as it involves a long-term investment problem associated for recovery and reconstruction.

2.3.1.5 Network systems

Resilience can be also defined for networks, besides systems and organizations. A network by itself can be considered as a system, or an organization may be represented by a network of systems. Wang et al. define resilience the intrinsic ability of the network to return to a stable or normal operating state following a strong perturbation or shutdown due to serious failure or outside attack [256]. For example, in a logistic network, its foundation function is to meet the requirement of all demand nodes. In the case of a disturbance, recovery of th network depends on the following three features;

- Redundant resources with adequate surplus to keep supplying the demand nodes, in the case of disruption.
- Supply from multiple resources, with inherent flexibility that is usually provided

by decentralized/distributed network architectures.

- Redundant supply lines with different levels of reliability. If cost is proportional to reliability, constant reconfiguration or resource allocation may ensure continuity of service at minimum cost, based on demand and supply figures.

2.3.1.6 Materials science

Before the concept of resilience was applied to systems, it's original definition was referring to materials and their strength under given conditions. Boyd defines resilience as the amount of work that is required to deform a unit volume of a material to the elastic limit. In other words, resilience is a measure of the energy that can be stored in a unit volume of any material and be then recovered as mechanical energy without any loss. In an alternative explanation, resilience is also considered as a complement of fragility, with the latter defined as the quality or state of being easily broken or destroyed [156].

2.3.1.7 Safety, security and risk

One of the most promising application of resilience engineering, is safety and survivability management. In fact, it is expected that more resilient system designs, result in improved safety and survivability. Along the lines of adaptability of resilient systems, Wildavsky defined resilience as the capacity to cope with unanticipated dangers after they have become manifest, learning to bounce back [262].

The U.S. Department of Homeland Security views resilience as an enabler for increased security. According to the 2008 DHS Risk Steering Committee, resilience is the capacity of an organization to recognize threats and hazards and make adjustments that will improve future protection efforts and risk reduction measures [99]. In particular, when security risks relate to terrorism, resilience is viewed as the capability of an asset, system, or network to maintain its function during or to recover from a terrorist attack or other incident [50].

From a survivability perspective, Castet interprets resilience as survivability plus the ability to tolerate unusual but legitimate changes, namely viewing resilience as a superset of survivability [39]. along the same path, Caralli [37] views resilience as a time dependent extension of survivability to include risk prevention and restoration of normal processes once a disruption has relented.

2.3.1.8 Systems Engineering and Architecting

From an architectural and systems engineering perspective, system resilience is not much different than safety management. In fact, resilience is more of an architecture characteristic than a safety feature. It is that some of the benefits of more resilient architecture are expected to contribute in improving safety and survivability. Allenby defines resilience as the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must [9]. From a systems engineering perspective, the primitive features of resilient systems are the ability to absorb change and disturbance, to maintain functionality, to adapt to change or gracefully degrade in natural and autonomous fashion, when it is necessary for the overall system survival and recovery. The U.S. DHS Risk Steering Committee supports this perspective, by alternatively recognizing resilience as the ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions" [99].

2.3.1.9 Stability and Control

Many researchers have argued and investigated the association between resilience and system stability. Even if stability is not an essential attribute of a resilient system, improved dynamic stability is one of the resulting benefits of resilient systems. In fact, the link between stability and resilience was part of earlier research towards defining resilience, based on ecology and environmental studies and extending to engineering applications. Gunderson defines engineering resilience as the speed of return to the steady state, following a perturbation [252]. Consequently, ecological

resilience is measured by the magnitude of disturbance that can be absorbed before the system is restructured [252]. From a dynamic stability viewpoint, resilience may be alternatively defined as the ability of a system or organization to react to and recover from disturbances at an early stage, with minimal effect on the dynamic stability" [111].

2.3.2 Revisiting safety management from the lens of system resilience

In accordance to Observations 2.1-2.3 and the Objectives set in Chapter 1, the overall goal is to investigate methods for improving system effectiveness, with emphasis on safety and system survivability. Given the limitations of SoA approaches within safety and survivability engineering, which were identified and presented in sections 2.1 and 2.2, the concept of system resilience is investigated within the context of the particular research directions. Resilience engineering is the enabling philosophy, in the sense that it addresses relevant issues in safety and survivability management, differently than traditional approaches. Such issues have been identified and discussed by the resilience engineering community[109]. These refer to diversity in understanding of safety, performance variability, accident occurrence, event development, risk assessment and they are summarized in Figure 49.

2.3.2.1 Performance conditions

Traditional safety engineering approaches follow the assumption of completely specified performance conditions. Assessments and safety tests are performed in isolated laboratories, where system operating conditions are fully under control. In that case performance conditions are also completely specified. However, real operating conditions are often not controllable, thus resulting to unpredictable performance conditions.

The uncertainty in operating conditions, refers to changing mission expectations

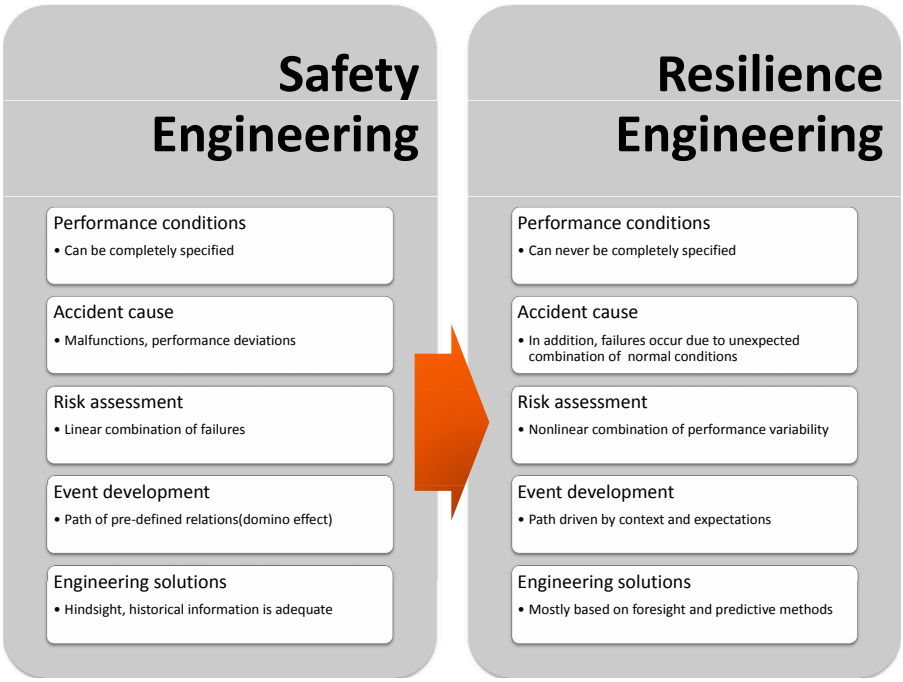


Figure 49: From safety to resilience engineering [109]

and to changing environmental conditions. The latter is also known as *operational uncertainty*. On the other hand, there is uncertainty in the system's ability to maintain its physical shape, its internal component connectivity and its mission configuration, relating to design faults and is known as the system's *design uncertainty*.

System complexity is a significant contributor, affecting both operational and design uncertainty. Performance variability is a natural consequence of system complexity. Effects of complexity stem from subsystem interconnectivity, emergent and unpredictable behaviors, or combinations of the previous [38]. If a system is comprised of a large number of components with well defined roles and governed by well understood rules, it is then referred to as a *complicated system* [10]. On the other hand, when a system of the same size is comprised by a set of components that their properties are not clearly defined or explained, exhibit nonlinear behaviors and are interconnected through a large number of connections, then this would be referred to

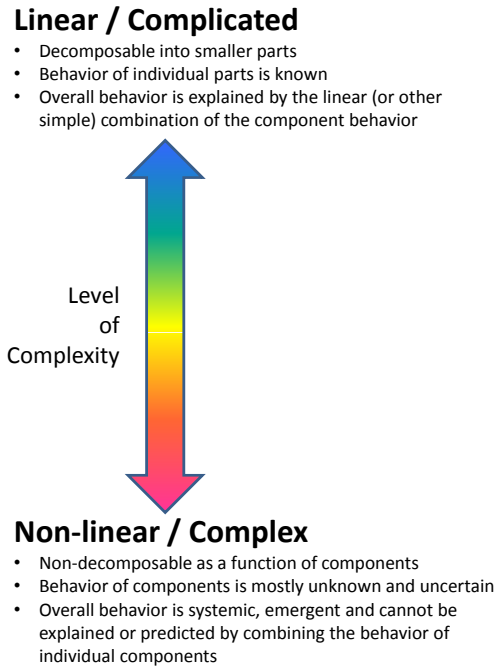


Figure 50: Impact of complexity in system behavior

as a *complex system*.

Performance variability may lead to system instability or even disastrous outcomes and therefore it is necessary to understand the nature of variability (why, when, how) in order to limit its effects [109]. Figure 50 illustrates the tradeoff between types of system coupling (interconnectivity) and levels of system complexity. Complexity-coupling tradeoffs are essential for better understanding of total system behavior, as well as discovering possible modes of failures and monitoring damage propagation.

The issue of varying and uncertain performance conditions is addressed by the concept of robustness. *System robustness* is defined as the insensitivity of system value delivery to changing contexts [190]. Given the uncertainty in system operating conditions and any possible disturbances (also known as "noise") affecting system design performance, the robust design solution is the one which is less affected by noise [158].

As dynamic systems become more complex, performance variability is expected

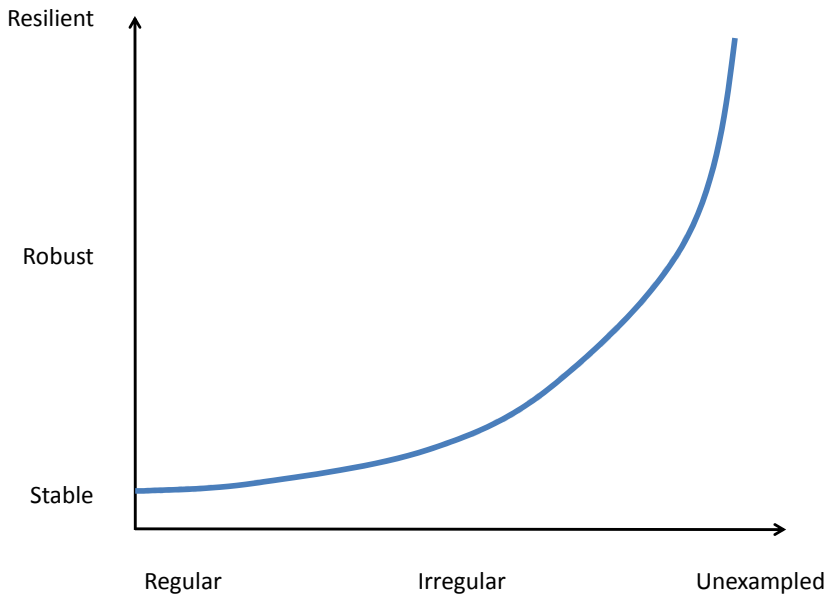


Figure 51: From stable to resilient [128]

to be unpredictably affected. Figure 51 explains the transition from stable systems to more robust, as performance conditions become more uncertain and less predictable. Resilience engineering advocates that systems not only should be insensitive to irregular, but also to unexpected and unexampled events. A system that is robust by design, is naturally insensitive to changes. To address however unexampled and any other unexpected events, a system must additionally be adaptive to changing conditions, mission requirements and any other physical changes that may occur on itself. This is a distinguishing factor between robustness and resilience, despite of the many similarities that researchers have been attributing to the two concepts [69]. Thus, system adaptability as an intrinsic architecture property is the basis for extending the concept for system robustness to system resilience.

2.3.2.2 Accident cause

Accidents are triggered by failures, which are further originated by faults on system functionality. Regardless of fault occurrence, most systems are able to function properly until they completely fail due to a certain or unexpected reason. Traditional

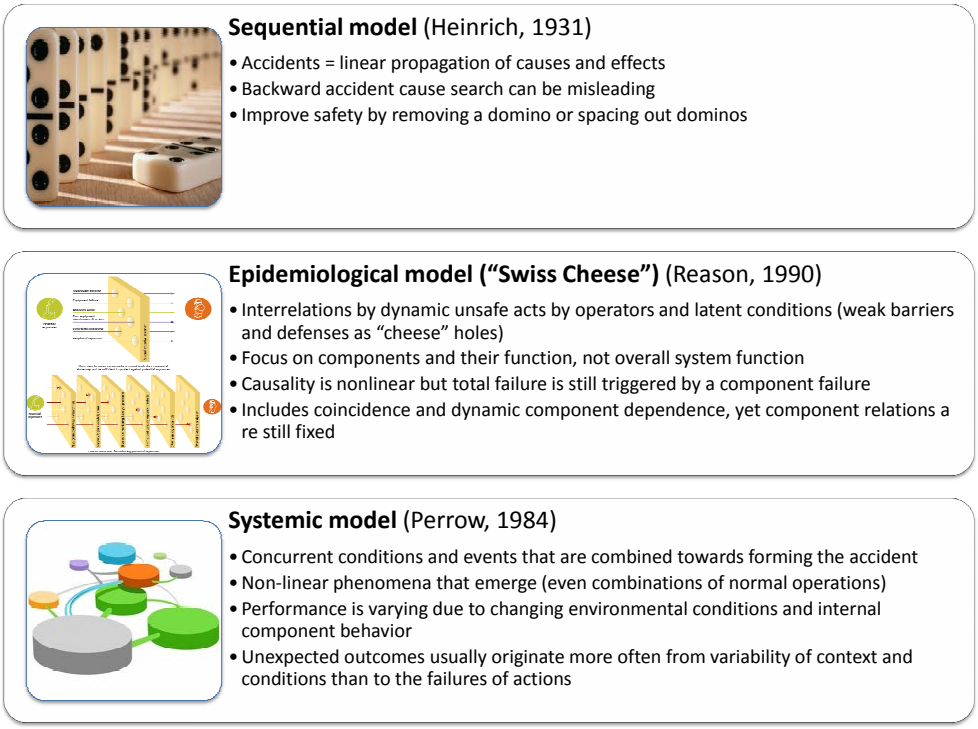


Figure 52: Accident models

safety engineering practices link failures to system malfunctions and performance deviations from normal operating states. Resilience engineering extends these practices by bringing the perspective of internal component complexity and coupling, for accident reasoning, including cases with no starting fault or damage. Under this view, performance variability must be regulated, unwanted combinations of component performance variability must be identified and suppressed, for the purpose of preventing functional resonance effects [110] or other adverse behaviors.

Depending on internal system complexity, three fault propagation mechanisms have been identified, and are represented by three behavioral models, simple linear, complex linear (complex subsystems linearly associated) or complex nonlinear. The corresponding accident models for capturing fault propagation, are the *Sequential* model [104], the *Epidemiological* model [186] and the *Systemic* model [176] respectively, as shown in Figure 52.

In the *simple linear system* accident model, the sequential ("Domino") model explains accidents as a linear propagation of causes and effects [108]. It is noted however, that backward accident cause investigation can be misleading, since an effect may have multiple causes [104]. To ensure safety, this approach suggests that a "domino" must be removed or effectively the system must be designed in such way that this abstract representation would correspond to more spaced out domino.

In *complex linear system* models, damage is predicted through a stochastic combinatorial approach, when the manageable risk of failure of a single component is given. The epidemiological ("Swiss Cheese") accident model was introduced by Reason, addressing the interrelations of dynamic unsafe acts by operators and latent conditions. The "holes" in the cheese represent weak barriers and defenses [186]. However, the model's main focus is on components and their function, ignoring any emerging behaviors on the overall system functions. While causality here is nonlinear, total failure is exclusively triggered by component failures. Phenomena such as coincidence and dynamic component dependence are considered, yet component relations are still fixed and unchanged over time.

Finally, in *complex nonlinear system* models, systemic accident models consider resonance effects and emergent behaviors of linked components. Systemic accident models take into account concurrent conditions and events, which if combined they result towards accident occurrence [176]. These conditions trigger non-linear phenomena that emerge during system operation (including combinations of normal operating conditions), while system performance is varying due to changing environmental conditions and internal component behavior (Exogenous/Endogenous variability).

2.3.2.3 Risk assessment

A third point that supports the paradigm of resilience engineering, is the view of accident risk, for the purpose of risk assessment. To effectively assess risk, the impact

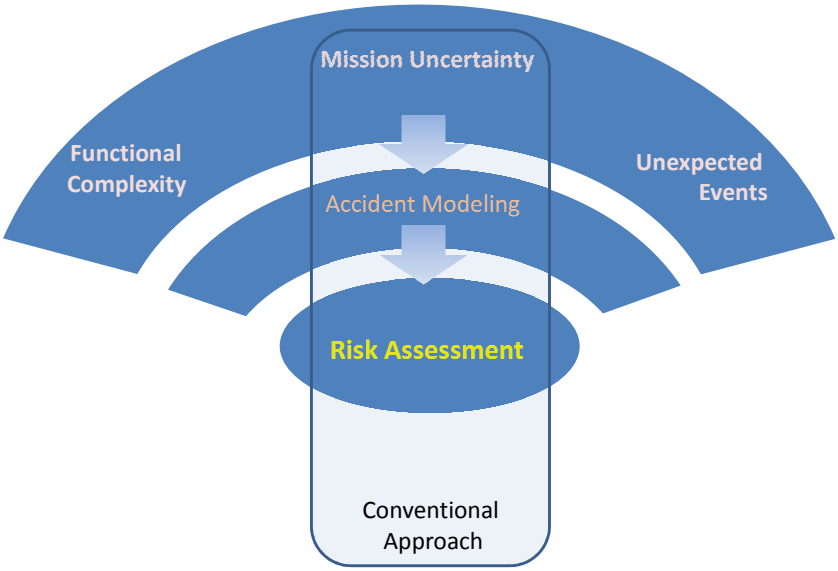


Figure 53: Fundamental steps for Risk Assessment [109]

of a threat must be predicted, thus accident modeling is a significant enabler for understanding the functional complexity of the system, which in turn determines the path to failure [109]. The fundamental steps of traditional risk assessment procedures, shown in Figure 53, depend on the accident model. Traditional safety engineering has adopted the linear accident model, namely assuming a starting fault, that can lead to failures and to larger scale accidents. However, it is not guaranteed that unexpected behavior, or other effects of increased system complexity are captured.

System resilience is founded on the alternative understanding of how system threats, result to accidents and how damage propagates, under unexpected behaviors, or other effects of increased system complexity. All complex dynamic systems exhibit a certain level of performance variability. It is assumed that mission or system failure, or success are all determined by the nature of this variability [109]. As the levels of performance variability increase, it is presumed that the risk of failure due to adverse effects, emerging behaviors and cascading failures is increasing as well.

According to Hollnagel, failure or success are the two sides of the same "coin",

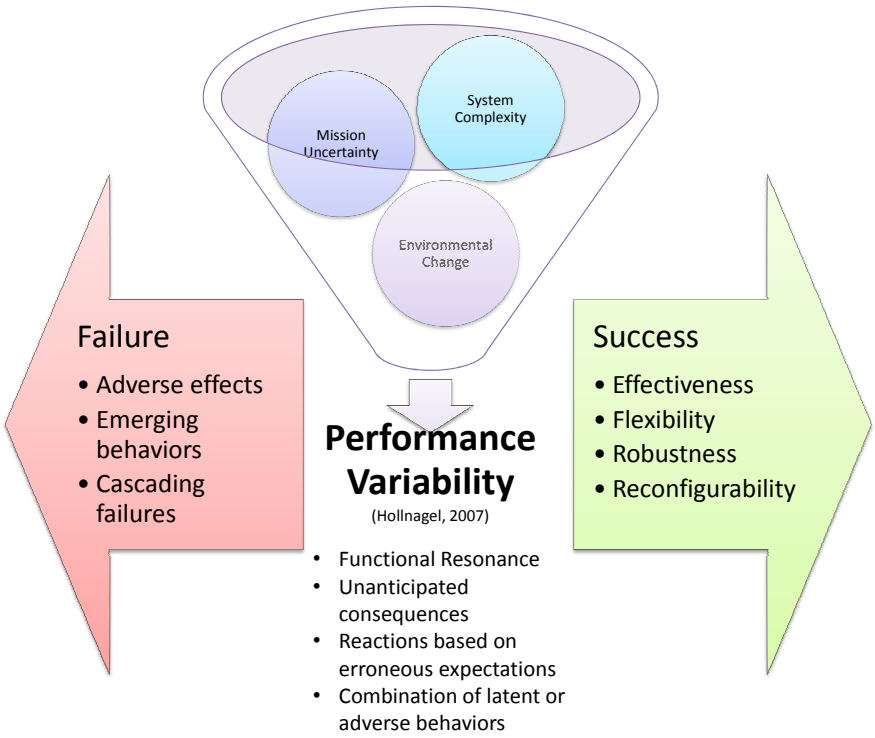


Figure 54: Performance variability to explain system failure and success [109]

which is performance variability, as Figure 54 suggests. In this context, "failure" is viewed as an inability to adapt to perturbations and unexpected events, rather than just a regular breakdown or malfunction [146]. To avoid failure, the system must be flexible, effective, robust and reconfigurable, implying lower, but nonzero levels of variability for mission success. Increasing system performance variability that could lead to failure is sourced by mostly nonlinear phenomena, such as functional resonance, unanticipated consequences, reactions based on erroneous expectations, or a combination of latent or adverse behaviors [110].

2.3.2.4 Event development

Strongly tied to accident models, as well as their application for performing risk assessment, is the understanding of how certain events take place, that could lead to either a failure or accident, while varying the levels of risk exposure for dynamical

systems. Thus, event development is another departure from ways of thinking within traditional safety engineering. Resilience engineering suggests the impact consideration of the environmental conditions and effects of complexity, as opposed to linear pre-defined paths for event development [214].

With simple system failures (e.g. a light bulb), it is possible to restore full functionality and system health, by just replacing the failed component with a new one. In simple systems, components are linearly interdependent, without emerging behaviors after a single point failure. Moreover, all component interactions for simple linear systems can be entirely explained, without any uncertainty. Thus, simple system performance is essentially *bimodal*, where either the system works correctly (as designed) or it completely fails. The final performance outcome on the other hand, is the product of a known path, which is determined by components interactions (similar to a "domino" path).

Unlike traditional views of safety for simple systems, with resilience engineering system performance is non-bimodal and safety is determined by the bandwidth of system performance variability. Given that performance variability is also dependent on operating conditions (context) and mission expectations, safety is a complex function of multiple factors. This includes unknown factors due to emergence of unexpected behavior, possibly driven by subsystem cross-connectivity, multi-level hierarchies, complex logic and non-linear coupling, all of them being typical effects of complex, large scale systems.

This alternative view of event development, is consistent with the *systemic* view of failure occurrence and propagation. Safety is now dynamically determined, with performance barriers that are not globally fixed, but are functions of real time operating and environmental conditions. While performance variability is necessary, as explained in Figure 54, systemic failures cannot be prevented by just restricting performance variability. The latter approach may prevent failures due to "domino"

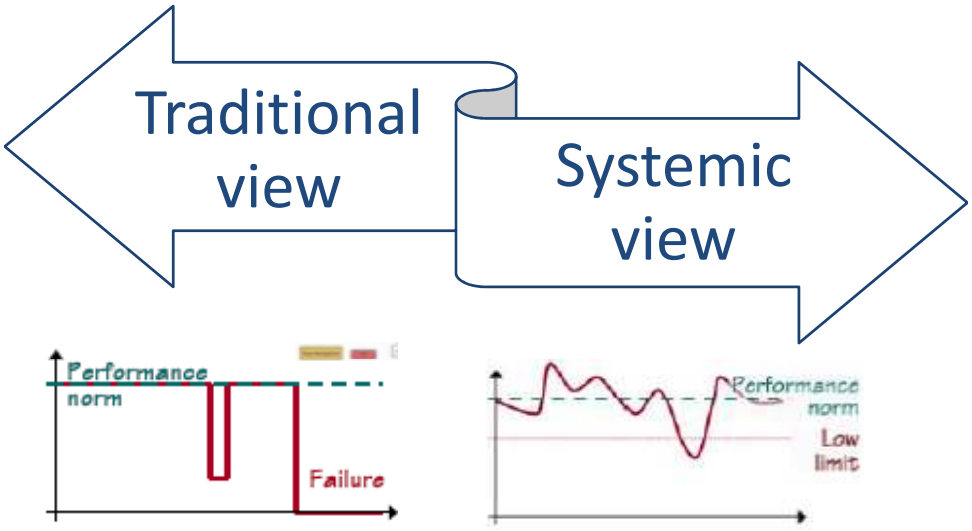


Figure 55: View of how failures happen ([109])

or "snowball" effects, however other failure modes can emerge due to subsystem connectivity combinations, even if all operate under normal conditions, and under total absence of earlier faults or failures. An overview of the event development concepts relevant to system safety is provided with Figure 55.

In support of better understanding of mechanisms for unexpected complex system behavior, the *functional resonance* model is introduced [110]. This approach draws parallels to systemic event development due to emerging behaviors, to resonance effects in second-order mechanical systems. The resonance effects induced on a small bridge, which is being crossed by a group of people marching at the same pace, is a simple example to illustrate this point. While the bridge is rated to withstand the weight (sum of all components), it appears that with the total weight unchanged, the bridge can collapse (lack of resilience) if marching induces resonance effects that degrade the weight rating (emergent behaviors) and make it effectively lower (effective weight sum that the bridge has to withstand becomes larger than the weight rating).

The presence and intensity of emergent, nonlinear and non-deterministic behaviors is representative of overall system complexity. A qualitative measure of complexity is

the difference in the behavior of a large scale complex system to the behavior of the equivalent sum of all components of the original complex system [38]. Another way to assess system complexity is through system *fragility*. System fragility is a property related to the system's brittleness. Fragility is used to describe infrastructure components in civil engineering or computational algorithms and networks in computer science and engineering, and is generally the complement of resilience [124].

Other notable complexity characteristics are the system's buffering capacity, its self-restructuring capability, and its natural ability to adapt against changing environmental conditions [109]. Buffering capacity refers to the size or disruption type that can be absorbed/adapted to without fundamental breakdown in system performance or structure. In other words, it depends on system design features or technologies that allow the system to naturally withstand most types of disruptions. With their self-restructuring capability, complex systems should not only be able to withstand disturbances, they must additionally be capable of returning back to normal operational status and complete the mission. Complex system adaptation, even though possible at local system levels, it is observed as a collective total effect, as part of the system's natural response to changing environmental conditions.

2.3.2.5 Engineering solutions

In safety engineering, there is strong reliance on engineering hindsight, and historical information, regarding risk and uncertainty around system operations and performance. While this approach is adequate for conventional designs and for mostly expected operating conditions, it is not always appropriate for large scale, complex and revolutionary concepts that often operate in uncertain operating conditions. It a quite challenging task to ensure safety by design, while more information is required to design more capable systems under such conditions.

Within resilience engineering, the above limitation is recognized and designing

complex systems, based on foresight and predictive methods is greatly advocated for. Foresight is pursued through real time simulations which offer insight regarding the system's dynamic response. High fidelity dynamic physics-based models are major enablers for response prediction and furthermore for design uncertainty reduction. This approach results in computational Modeling & Simulation (M&S) environments, that represent large scale system architectures and are capable of predicting a system's dynamic behavior under changing conditions. Beyond design uncertainty, further steps can be taken to address operational uncertainty, which stems from operating environment risks. Resilience engineering supports the need for improved situational awareness [75], essentially the system's capability of properly sensing and assessing changes in its surroundings, reflecting mission and environmental uncertainties.

2.3.3 Applications in resilience engineering

Resilience engineering has proliferated as a paradigm shift in safety management, and has been investigated for several different system applications. With system safety as one of the core values that this discipline seeks to address, resilience engineering is envisioned to become an ecosystem of basic principles, definitions [156], assessment and analysis techniques, modeling approaches and design methodologies [146], [114], [211]. The fundamental research initiatives within the practice of resilience engineering, have been focusing on the following methods and tools [249]:

- Analysis, measurement and monitoring of system resilience in their operating environment.
- Improving system's resilience.
- Modeling and prediction of short and long term effects of change, while formulating and selecting management decisions on resilience and risk.

In an overview of today's State-of-the-Art in resilience engineering, significant progress has been made on understanding and clarifying the concept for different applications. Some of the most common applications are:

- Dynamical systems [54].
- Complex networks [142], [95].
- Organizations [13].
- Materials and structures [160].
- Infrastructures and communities [117], [71].

As the need and interest on resilient systems further advances, government agencies are working on policymaking and requirements formulation on resilient large scale organizations and infrastructures [52], [91], [13]. In terms of method and tool development, the literature search has indicated numerous resilience assessment techniques [71], resilience improvement techniques and technologies [149]. Last, modeling approaches for resilience analysis address system functionality, complexity in system architectures and interconnectivity, as well as performance and effectiveness.

A complete proposal for a resilience-based design methodology has been introduced through the Resilience for Survivability initiative by IST (ReSIST) [19]. It's a collective attempt towards a quantitative methodology for resilient complex systems, while maintaining a high level of generality. At the same time, ReSIST offers its own view of resilience engineering, through their definitions and assessment framework.

Richards, et. al, as part of MIT's SEARI Initiative, has introduced a dynamic multi-attribute tradespace exploration technique [190], which despite its focus on system survivability, it does bring ideas that are compatible to resilience engineering. The demonstrating application is a satellite under possible degradation, which is

maintainable during its mission, thus exhibiting dynamic recoverability through its design configuration.

The Idaho National Laboratory (INL) has been working on a Resilient Network Design Environment (RNEDE), through which it intends to visualize, Create, Edit and Analyze large complex networks/graphs [248]. Principles of resilience engineering are implemented for complex network architectures. Within RNEDE, a dynamic simulation platform is utilized for the development and resilience evaluation of networked system control strategies. The simulation environment (RNEDESim), supports the method with multiple capabilities, such as scalability, threat and disruption scenario playback, recovery option suggestions, network visualization, while it remains application-independent. The method returns a certain topology, which satisfies a set of constraints, while minimizing a cost function against a series of incidents (disruptions), and performs tradeoffs between remedial options and the cost function.

The resilient design methods survey concludes with two other approaches. The Resilient Industrial Control System (RICS) design method is based on an application specific formulation of concepts and metrics for resilient telecommunication systems [257]. Last, another effort concentrates on resilient design of recharging station networks for electric transportation vehicles [250].

2.3.4 Evaluation of resilience engineering approaches

Resilience engineering has been inspiring several researchers and agencies to further understand and investigate this new emerging discipline. As the literature has indicated, the problem of designing resilient systems is addressed from different aspects, such as requirements for system resilience, policies, assessment techniques, technologies for resilience enhancement, and to smaller extent, resilience-based design methodologies. Figure 56 presents an evaluation of SoA methods in resilience engineering.

In current SoA approaches, the lack of design techniques with system resilience

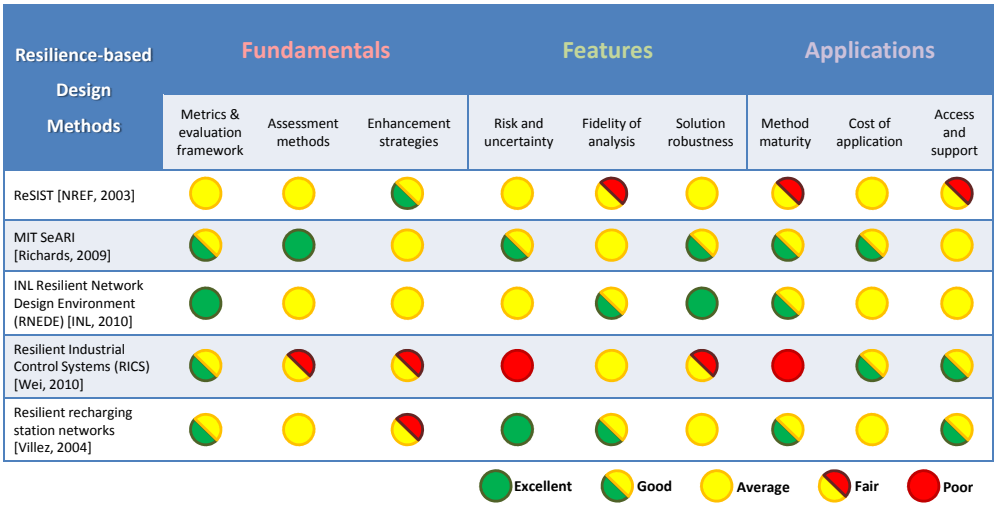


Figure 56: Evaluation of resilience-based design methods

as an objective function, is the most observed gap and ongoing research efforts are already addressing it [251]. Most approaches focus on requirements, policies and assessment methods.

Observation 2.10: For most applications in science and engineering, resilience-based design methods are still at their infancy stages. Most of them qualitatively address the problem of resilience, through requirements for ideal resilient system response, enhancement recommendations and policies formulation towards more resilient systems.

According to common scientific practices, before one can design a system to adhere to certain objectives, and that is subject to particular constraints, one must be able to evaluate system performance and behavior against these requirements. Assessment techniques are thus a major method building block and the SoA review has confirmed recent efforts towards system resilience evaluation and assessment.

Observation 2.11: Resilience assessment techniques are currently the main focus of the resilience engineering community, as they would be one of the basic building blocks for resilience-based design methods.

As it may be quite early for validated resilience-based design methodologies, a few SoA approaches seek to utilize well established design techniques, in support of designing more resilient systems. For instance, robust design [177] and strategic decision making for technology infusion [131] are techniques in support for more survivable and effective systems. However, incorporating advanced capabilities are expected to implicitly benefit system resilience to most external or internal threats and disturbances. Furthermore, discipline based approaches, such as applied control system design [98] and resilient controls [194], are techniques for system adaptability and mission reconfigurability, that are expected enablers of system resilience [109].

Observation 2.12: While there are no validated techniques for resilience-based design, research initiatives have been resorting to well established robust design, optimization, applied controls and decision making techniques, to implicitly improve system resilience.

2.4 Complete problem definition

Recognizing that the research problem that the present dissertation is addressing is quite broad, it is necessary to scope the problem to a concentrated version, which will be better suited to further exploration and experimentation. The main motivation, as introduced with Chapter 1, is the investigation of systems engineering and methodologies for the design of more effective and capable systems. More emphasis was brought on safety management and how the problem could be formulated from a survivability standpoint. This present chapter has offered the necessary background information, regarding today's SoA approaches in safety and survivability engineering, as well as future directions with great potential, such as resilience engineering. A similar SoA investigation, along with the discussions on resilience engineering have been the basis of the potential contributions towards more effective systems, under the presence of operational uncertainty and system complexity.

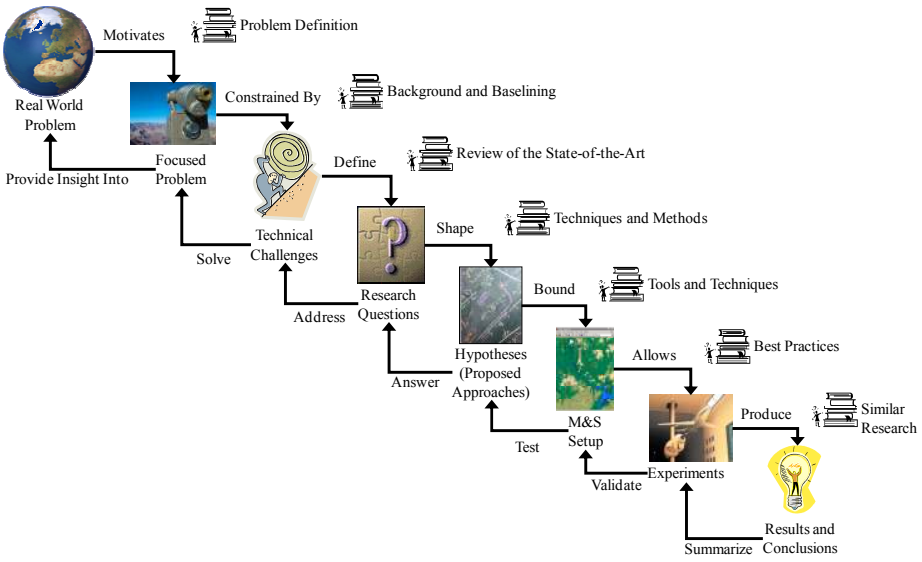


Figure 57: Scientific method for engineering research [151]

2.4.1 Revision of observations

Literature review on safety management, survivability and resilience engineering has allowed for several observations regarding the current State of the Art (SoA). These findings will be the basis of expanding Objectives 1 and 2, to a set of more concentrated objectives and a complete, focused problem statement for this dissertation. The development of the research curriculum is in accordance to the scientific research process [151], and is shown in Figure 57.

The two introductory research objectives, as stated in Chapter 1 are:

1. **Objective 1 (Main)**: Invest towards conceptual design methodologies that improve system effectiveness through increased survivability.

2. **Objective 2**: Follow the vision of resilience and investigate options on how resilience engineering can be implemented in advanced design methodologies with safety management concepts as objective functions.

The SoA investigation on safety engineering, survivability-based design, and resilience-based design methods, has returned a series of observations, which along with Observations 1.1-1.11, are summarized in Figure 58.

Observations 2.1 to 2.3 refer to SoA in safety engineering. Safety engineering is good resource for leveraging methods and techniques, which refer to problems that resilience engineering is also seeking to address. Safety requirements by military and certification standards, are valid resilient system requirements, however, these should adapt to visionary concepts that the resilience engineering community seeks to explore. As safety assessment techniques, such as PRA, FTA, and FMEA are at the most advanced level in their history of application, they could become significant enablers for design space exploration for resilient concepts. As a result Objective 2, can be further expanded to account for these new findings. **Objective 2.1**: Incorporate valuable safety management analysis and assessment techniques (e.g. PRA, reliability analysis, FTA, FMEA) for addressing risk and uncertainty in expected, yet adversary operating conditions.

Similarly, Observations 2.4 to 2.9 seek to reflect the SoA in survivability-based design. Survivability is a step closer to system resilience, than system safety, in the sense that the system must preserve itself and its mission under the occurrence of disturbances in a timely manner. Following Objective 2:

Objective 2.2.1: Explore the concept of resilience in conjunction to system survivability

There are several effective survivability-based design methods, yet most are specific to the application they were developed for. As in safety management, assessment techniques are the backbone of survivability design methods, both for analyzing the system's response to threats, or to allow for design space exploration as a method enabler. Survivability is a probabilistic measure that accounts for risk and uncertainty,

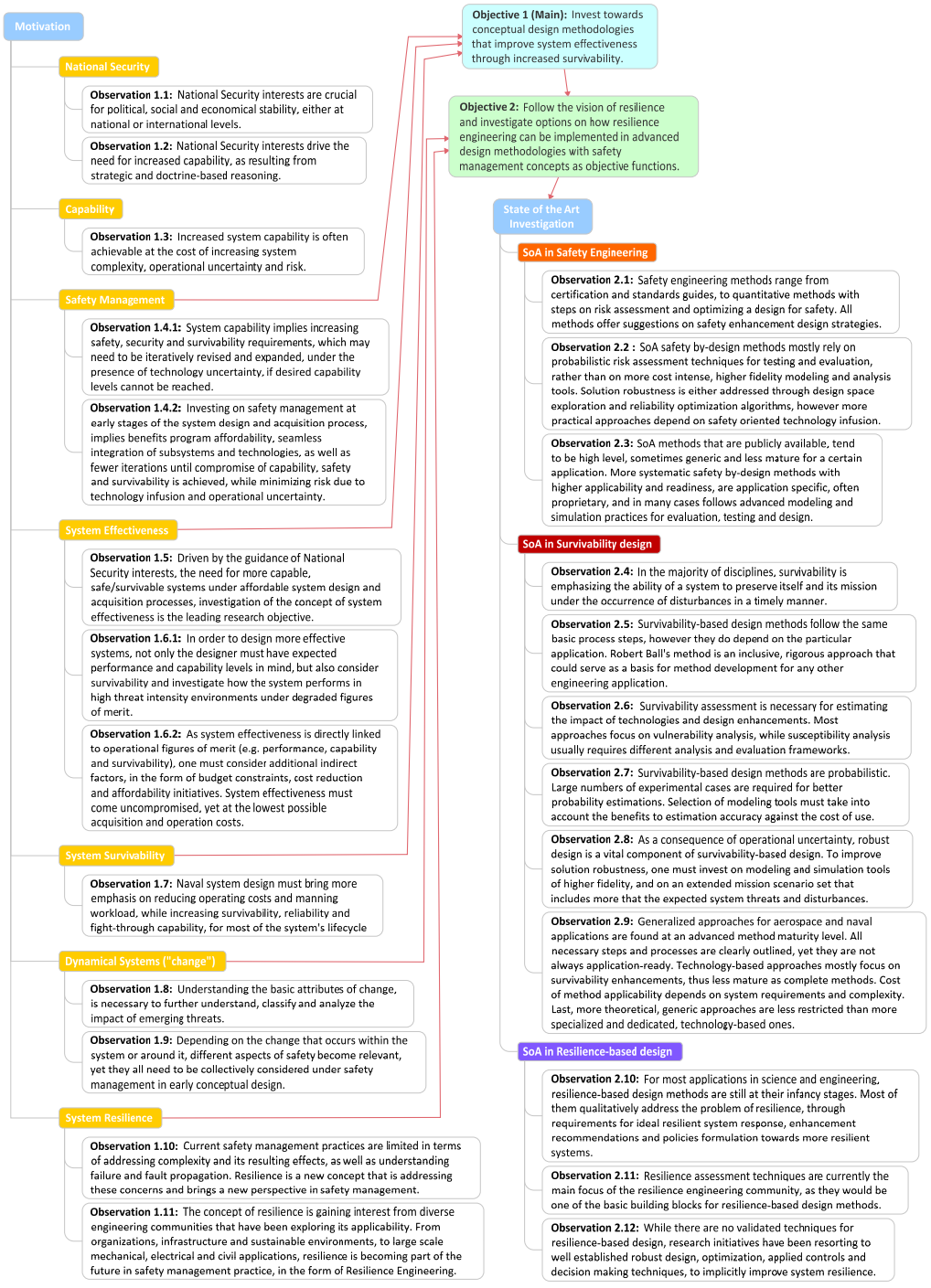


Figure 58: Summary of observations

thus most methods rely on probabilistic techniques, statistical analysis and multiple experiments.

Objective 2.2.2: Investigate the applicability of survivability-based design techniques to applications in resilience engineering.

System robustness is implicitly evaluated through survivability and is either achieved through intelligent design solutions or technology infusion.

Objective 2.2.3: Clarify the associations between system survivability and robustness, while investigating how robustness is related to system resilience.

The last set of observations, Observations 2.10 to 2.12, involve the SoA in resilience engineering. Resilience-based design methods are still at their infancy stages. It has been also observed that most research efforts are focusing on better understanding and defining the ideal resilient system response according to the resilience concept. As a consequence of the early stages of resilience engineering, resilience assessment techniques are currently the main focus, as they would be one of the basic building blocks for resilience-based design methods. Therefore, accepting that system resilience assessment is indeed, a natural prior step before fully capable resilience-based design and optimization methods, the ultimate objective for this dissertation is:

Objective 2.3: In support of resilience-based design methods, a system independent resilience assessment methodology must be developed.

2.4.2 Problem description and application of interest

Objectives 1 and 2 to 2.3 are the basis of the research direction for this dissertation, which will focus entirely on the development of *a theoretical framework for a resilience assessment method*, as summarized in Figure 59. The main set of deliverables for this effort is a suite of tools, methods and techniques related to resilience assessment and

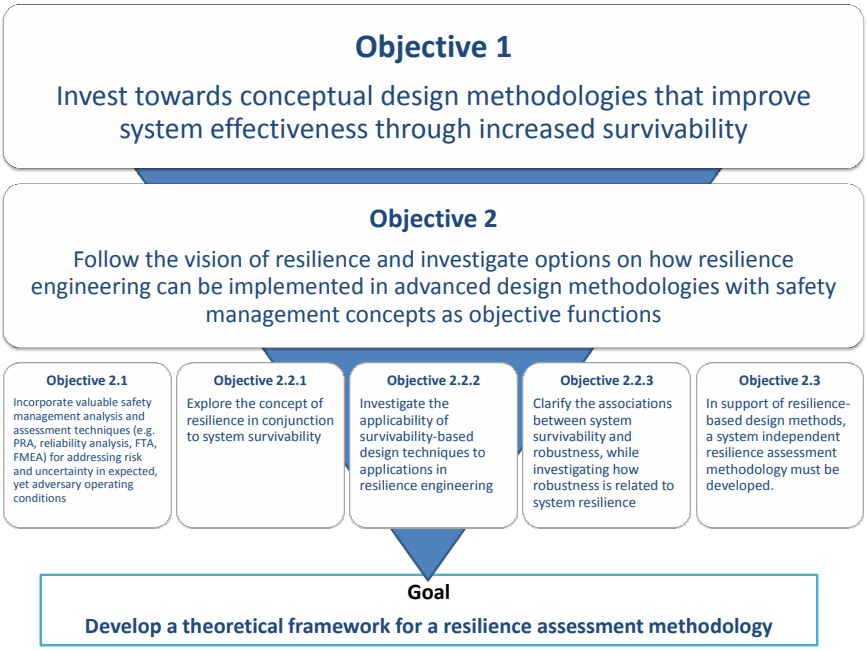


Figure 59: Problem Statement - Main goal and objectives

improvement. Along this path, the ultimate future goal is to employ this theoretical framework in systems engineering and incorporate these enabling techniques into complex system design methods. By this, not only resilience will be incorporated into formulating policies on system safety and survivability, but also business planning practices could be effectively supported [251].

From an application perspective, the long term goal is to investigate how can naval systems be engineered so that system effectiveness and survivability are maximized, through enhancing inherent system resilience. As discussed in the previous chapter, the need for more effective naval systems dates back to early 2000, and has been popularized through the US Navy's IEP vision [144]. The Aerospace Systems Design Laboratory (ASDL) at the Georgia Institute of Technology has introduced the IRIS concept in response to the IEP vision [253].

An IRIS designed ship will be *self-monitoring*, *self-assessing*, *self-reacting* and *efficient* as determined by IEP initiatives and technologies [115]. Self-monitoring will enable continuous sensing of all ship-related operations and encourage a system that is knowledgeable of both current and impending failures. As a self-assessing system, the IRIS ship will collect input data from all subsystems and sensors and either automatically diagnose and act on the best course of action or pass the information to a human/robot decision-maker. The self-reacting feature will allow the resources and commands to be distributed as necessary and prepare to compensate and continue to function in the event of system failures. In short, this integrated system and technologies onboard will have the ability to automatically *sense*, *assess* and *react* to changes in constantly changing scenarios, in support of the envisioned IRIS operations.

For the sense function implementation, an IRIS-designed ship will contain a network of system sensors for tracking ship motion, monitoring personnel status, detecting damage, monitoring machinery health, and evaluating weapon system readiness. Each ship subsystem will contain sensors to monitor its respective health status. This includes power, fluid (fire mains, seawater, fresh and chilled water, fuel and air systems) and damage control, and other critical systems which will utilize the advanced network of sensors [70]. Damage control is implemented through fire suppression and relies on automated valve and pump status control, for damage isolation, and available resource reconfiguration for optimum continuous operation (e.g. as in the Reduced Ship Crew through Virtual Presence (RSVP) demonstration [210]). Other sensors, e.g. Personnel Status Monitors (PSMs), can be used to monitor crew health status remotely during times of crisis.

On the assess function, IRIS must automatically analyze and assess the data from the sensors and identify the methods for avoiding or mitigating any foreseen problems. Despite the load of real time data, the information must be rapidly assessed. A distributed intelligence system will reduce the dependency on human operators, while

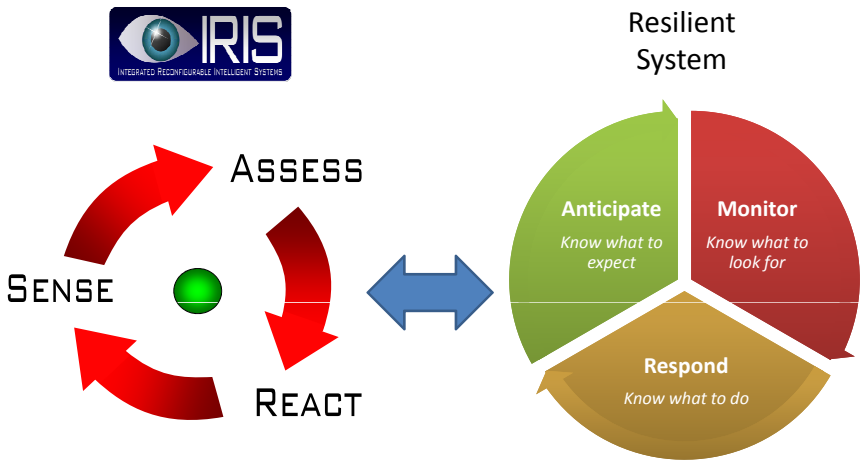


Figure 60: IRIS and system resilience

reducing operating cost and increasing efficiency [70]. As an autonomous system, the ship's attack systems are enabled [1], while onboard operators will directly interact with a visual, top-level interface with on-demand access to additional information [144]. When the data are neither accurate nor available, the system has to be able to infer what the state is.

The react function takes advantage of the distributed intelligence system and the controllers onboard, to physically reconfigure the different ship modules based on the sensors and the assessment of the information [5]. For instance, sensor information will be used to determine the optimum alignment of the ship given the subsystem health information and any predicted failures in the near future. Possible reconfigurability strategies would isolate subsystems from remote failures, by rerouting power, fluid flow or data through redundant paths to avoid cascading failures.

In conclusion, one may wonder how relevant is the concept of resilience to what an IRIS system is envisioned to perform. In many ways, IRIS is an implementation of a system that must be resilient to many threats and unexpected events, and that should be manifested through increased survivability, reconfigurability and adaptability to environmental changes. As resilient systems must be characterized by properties, such

as adaptability, self-healing, mission recoverability, safety and security, an IRIS system seeks to be similarly characterized, by employing advanced controls, intelligence and autonomous operations. Indeed, both schemes of the "sense-assess-react" in IRIS and the "anticipate-monitor-respond" of a resilient system, describe the iterative process that an adaptive, autonomous and self-reconfigurable system must execute for maintaining operations and minimizing impact of adverse effects. Thus, even though functions are not the same, the end functionality is equivalent, as suggested by Figure 60. However, it is an open challenge to experimentally demonstrate that a system which is designed as an IRIS system, is actually resilient, and this is one of the goals for the resilience assessment framework that is being developed through this research work.

CHAPTER III

ASSESSMENT METHODS IN SAFETY MANAGEMENT

Chapter 2 initiated a multi-disciplinary literature survey on safety management, survivability and resilience-based design methods. Based on a series of Observations, it has been concluded that the backbone of a resilience-based design method, would be a system and discipline independent resilience assessment technique, which allows for system resilience evaluation, under the presence of uncertainty and changing operating conditions. This present chapter is presenting a subset of the research survey, which concentrates on assessment techniques for safety, survivability and resilience, across different disciplines and applications. The literature survey for the assessment techniques aims to identify the strengths of current approaches, the detriments and technical challenges, along the path towards a set of research questions, the upcoming research opportunities and the experimentation plan for this dissertation.

3.1 Safety assessment methods

Assessment techniques in safety engineering are based on procedures that aim to quantify risk and provide reliability estimates, when certain uncertainty scenarios are given. Historically, safety assessment techniques were initially applied for civil aviation vehicles, as well as military systems. As safety became a major attribute of interest on other applications, safety assessment methods have been adopted for space, marine, automotive and civil engineering systems.

3.1.1 Methods survey

The U.S. aerospace industry has been a pioneer in safety engineering and has thus influenced the procedures for assessing system safety. The SAE-ARP4754 Safety

Applications / Techniques	Military systems	Civil systems	Automotive	Public Health
SAE ARP4754 Safety Assessment process		✓		
EUROCAE ED–79		✓		
Probabilistic Risk Assessment (PRA)	✓	✓		✓
Quantitative/Qualitative Reliability Assessment		✓	✓	
EPA Risk Assessment				✓

Figure 61: Origin and application of safety assessment techniques

Assessment process is standard procedure in civil aviation [203]. The European aerospace industry follows similar directives on safety, with the EUROCAE ED-79 publication as the equivalent of the SAE-ARP4754. There is also the European Directive 89/392/EEC [63], along with documentation for strategies in selecting safety measures, based on risk analysis and risk assessment.

As safety is linked to risk and uncertainty, probabilistic approaches have been developed, such as the *Probabilistic Risk Assessment* (PRA) [220]. In other applications, safety is associated to reliability, thus qualitative and quantitative techniques are also available [129]. Last, the Environmental Protection Agency (EPA) is using their own risk assessment technique, for public health and human exposure to hazardous substances and materials [76]. In Figure 61, an overview of the most prominent safety assessment methods is presented, and classified against the applications, for which these methods were developed and used.

All assessment methods require the identification of all possible hazards and sources of risk. Given that risk can be quantified for known sources of uncertainty, it is possible to determine the acceptable risk levels, and further investigate other sources of uncertainty that are linked to unavailable or non-existent knowledge. Risk assessment provides estimates for the overall system safety levels, and further allows

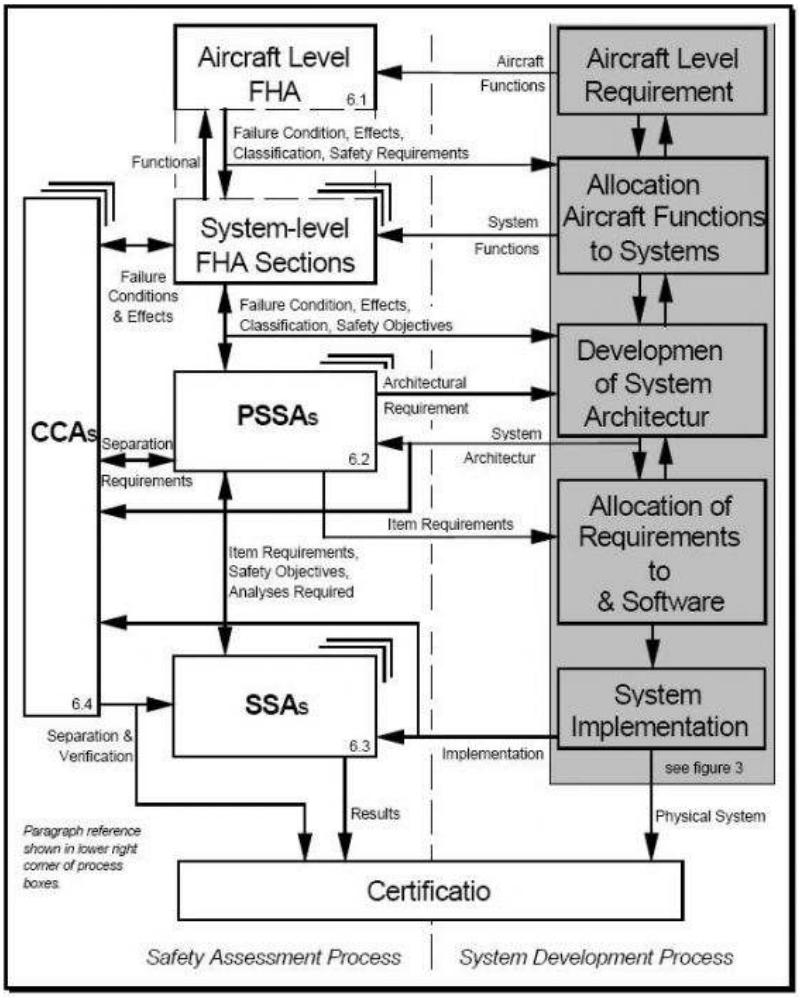


Figure 62: SAE ARP 4761/4754 safety assessment process model [203]

for estimating system reliability and availability.

There certain techniques for hazard identification that often constitute the building blocks for most safety assessment techniques. Common hazard identification techniques are Preliminary (or Failure) Hazards Analysis (PHA), Common Cause Failure (CCF) analysis, Fault Tree Analysis (FTA), Failure Mode and Effect Analysis (FMEA). Historically, fault trees were introduced by Bell labs [78] in 1961 to model missile reliability, while FMEA was introduced at McDonnell-Douglas [221]. An example on how these techniques blend together in a safety assessment process, is illustrated in Figure 62 for the SAE-ARP4754 safety assessment process.

Probabilistic risk assessment techniques rely on risk estimation for each hazard (extent of possible harm and probability of its occurrence). For large scale systems (e.g the Space Shuttle), several aspects must be considered, including persons exposed (operators and third parties), type, frequency and duration of exposure, human factors (man /machine interactions, ergonomic effects, etc.), and reliability of safety functions.

Reliability assessment techniques can be either qualitative or quantitative [254]. Their differences mostly concentrate on how the effects of a failure are modeled. Qualitative approaches employ Preliminary Hazard Analysis (PHA) and failure modeling is performed by:

- Failure Mode and Effect/Criticality Analysis (FMEA/FMECA)
- Fault Tree Analysis (FTA)
- Event Trees
- Cause-Consequence Diagrams

For FMEA, the system of study must be defined along with its main functions and components. Moreover, the functional limitations of the system and its components should be specified as well. Given that threats that cause malfunctions and failures originate from the environment, information must be provided regarding operation of the system, its components and the environment.

Quantitative methods are utilizing more advances modeling techniques for fault and failure analysis. Common techniques are:

- Fault trees (dynamic/static)
- Reliability Block Diagrams (RBDs)
- Markov chains

- Stochastic Petri nets
- Standard/custom simulation environments

The option for a custom simulation environments refers to failure modeling through dynamic simulation models (in Simulink, C++, Java, etc.). While not the most affordable option, the latter allows for more accurate prediction for failure and damage propagation throughout a system, through physics-based modeling and simulation. There are two possible ways for investigating the solution space, either form combinations of environmental conditions and mission requirements to obtain discrete sets of solutions, or perform a Monte Carlo simulation with random combinations.

3.1.2 Evaluation of methods

Starting from the hazard identification, fault and failure propagation analysis techniques, there are certain issues on their effectiveness that can be observed. Fault trees are top-level oriented. They focus on the "big picture" of the system, by often neglecting detailed subsystem and component associations, or assuming that these do not considerably affect the main failure effects. While fault tree techniques are adequate for less complicated systems, in the case of more complex or distributed large scale systems, they fail to capture possible emerging effects.

Observation 3.1: Fault tree techniques are capturing fault propagation, based on high level system information. They may not be as effective for more complex large systems, with extended low level connectivity and functional complexity.

Part of this inability, is the fact that they require explicitly prescribed scenarios as inputs, in order to predict how faults propagate. This approach offers no space for emerging behavior prediction. Last, the implied binary logic of two failure modes, either success or failure, does not allow for capturing the intermediate states that the overall system may find itself in. It also does not allow for accurately modeling

the actual contribution of a subsystem, in case it is characterized by more than two states, or a continuous spectrum for its operating modes.

Observation 3.2: Fault trees and reliability block diagrams heavily rely on initial fault scenarios and often lack flexibility in capturing transient and emerging effects, as they are binary in nature.

Fault trees, and reliability block diagrams are often ineffective when it comes to modeling dynamic complex system behavior, especially regarding reconfigurability, adaptability and maintainability effects. Static and linear causality logic is possible to be implemented, and for better fidelity in reconfigurability and logistics, Markov Chains and Petri Nets are better selections for fault and failure propagation analysis.

Observation 3.3: Fault tree techniques are often incompatible to models of complex system behavior, thus failure propagation prediction is static and does no take into account reconfigurability and maintainability effects.

Returning to the safety and risk assessment techniques, Figure 63 presents a qualitative evaluation of the SoA approaches that have been retrieved from the literature. The reasoning behind the selected criteria for method evaluation can be found in Appendix B, as in for the design method evaluation, that was included in Chapter 2. Regarding the basic features, most methods rely on comprehensive sets of metrics (e.g. SAIDI, SAIFI metrics on power plant reliability assessment), which are evaluated based on data collected after the system's response to a range of certain threat types and magnitudes. Given that most methods are standard in the industry or application of interest, it is safe to accept that they have been successfully verified and validated

It has been observed however, that the effectiveness of assessment methods does rely on how threats and disruptions are modeled. Standardized engineering assessment methods offer better detail on how disruption scenarios should be constructed.

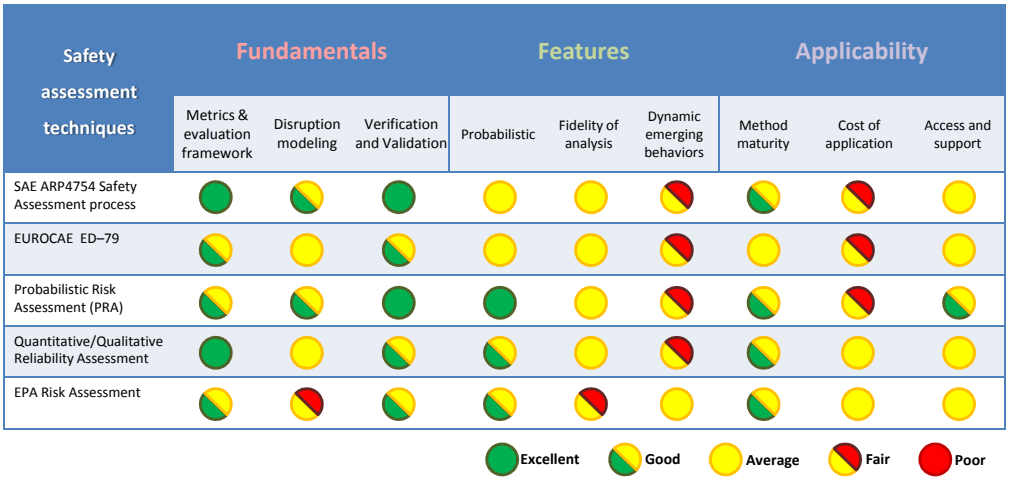


Figure 63: Evaluation of safety assessment techniques

On the other hand, disruption modeling is still scenario-based, not always allowing for accurate capturing of secondary, or emerging disruption effects. The latter feature, is dependent on the modeling approach and the fidelity of the simulation. As most methods are probabilistic, behavior variability is a result of the combinations number for the initial disruptions, rather than the different scenarios that will appear as a result of different emerging behaviors, for the same initial disruptions.

Observation 3.2.1: To avoid reliance on initial fault scenarios, more accurate, physics-based dynamic system models are necessary, in order to capture intermediate subsystem states and emerging behaviors.

In terms of method applicability, most methods possess an increased readiness level, which makes them effective for most of today's engineering applications. As many of them are based on government and industry standards, documentation, access and support are at a satisfying level, with the exception of methods that refer to proprietary systems, or revolutionary approaches in the industry. However, cost of application, either in the form of cost of testing, or time required to perform the assessments, there are no techniques without compromise in modeling fidelity or quality of the results.

Observation 3.2.2: The cost of more accurate, physics-based dynamic system models is higher than simple, static modeling approaches, thus there is a compromise between computational fidelity and method accuracy.

3.2 Survivability assessment methods

Assessment techniques for survivability-based design, are focused on survivability estimations, based on partial evaluations of system susceptibility and vulnerability. This section will present the most prominent survivability assessment techniques, used in military aircraft acquisition, as well for naval systems. As in safety and reliability assessment, survivability assessment techniques rely on scenarios, which incorporate the effects of threats during mission, or common sources of disruption and malfunction.

3.2.1 Methods survey

It has been argued that system survivability is an important requirement in military systems. Thus, most methods are based on military aerospace and naval system applications. A list of the considered assessment techniques is presented in Figure 64. Some of these methods are highly integrated and tailored to survivability-based design techniques, which are also specific to certain applications. However, this aspect does not reduce their value, given that some underlying principles are system and application independent. Certain limitations apply in the modeling approach for scenario execution, as well as in the availability of model or configuration information, especially when military systems are involved. Last, other techniques (e.g. MOTISS by Alion Technologies [8]) have been developed as stand-alone computational environments that can be used as independent sessions for any system application.

Techniques \ Applications	Aerospace systems	Naval systems	Automotive	Public Health
Robert Ball's & survivability assessment methods	✓			
SURVICE Assessment Technique	✓			
Total Ship Survivability Assessment (TSSA)		✓		
Survivability assessment by IMO		✓		
MOTISS [Alion, 2009]		✓		

Figure 64: Origin and application of survivability assessment techniques

3.2.1.1 Ball's assessment technique

Dr. Ball's technique has been an integral part of his survivability-based design method, with application on fighter aircraft [16]. It is a close representation of the methodology that has been adopted by the industry. Aircraft survivability can be assessed at the *campaign* level, with multiple aircraft sorties, or at the *system* level with a single vehicle at various environmental conditions and mission expectations.

The technique requires the mission profile and a threat encounter analysis to be initiated. A typical combat mission profile consists of phases, such as loiter, target search and acquisition, and weapon delivery during encounter between take-off and landing. Regarding threat characterization, a threat is described by its attributes (intent, direction, magnitude, etc.) and the operating conditions. A threat can demonstrate its malicious intent by deploying multiple damage mechanisms, as part of a system kill attempt, either operationally or physically. Operations around the threat, involves the series of functions that are executed for target kill. That is, searching for the target (search-detect-track) and attempting to kill by navigating the weapon(launch-fire-navigate), or just propagating the threat to increase system damage.

Returning to the main military system of reference, a functional analysis and

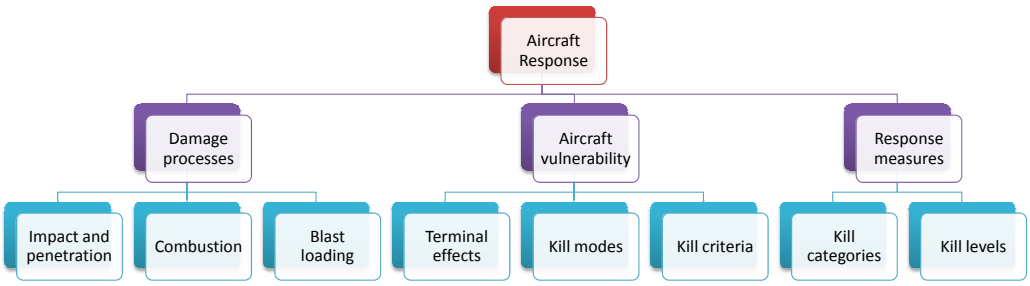


Figure 65: Elements of aircraft response to a threat [16]

decomposition is necessary. The system's essential functions must be identified, either for executing its mission or its basic operations. Fighter aircraft, must be capable of locating and engaging their targets, as part of their main mission, while maintaining their essential operating functions, which include the ability to provide controlled flight, maintain structural integrity, generate lift and overcome drag.

The next step is perform failure mode and fault propagation analysis. The focus is brought on analyzing how the system reacts and further behaves under the experience of a threat. As a means to investigate aircraft vulnerability, damage propagation modeling will indicate the kill modes for the identification of the damage states, through which the system may undergo. For the fighter aircraft example [16], vulnerability investigation requires particular measures for damage mode analysis, and these are presented in Figure 65.

Simulation results, which were produced according to the formulated mission and threat scenarios, are the basis for terminal effects and kill mode identification. Terminal effects represent the damage state of aircraft components that are subjected to damage processes, due to threat elements. Ultimately, after several terminal effects, the aircraft may experience a mission kill or even a system kill. A kill mode is defined as the component or system response that results in a component or system kill and possibly an aircraft kill caused by loss of an essential function. In other words, the kill of some critical components, such as the pilot or an engine, might result in a quick

attrition kill of the aircraft, namely *system kill*. The loss of other critical components, such as a navigation computer or weapon sensor, can result in a mission abort kill, or *mission kill*, because the pilot decides to return to base before achieving the mission objectives. A list of components that are subject to terminal effects and can result to kill modes is shown in 66.

With the mission and threat analysis tasks leading to kill mode identification, the subsequent steps command for the quantitative susceptibility and vulnerability analysis. With a clear picture of the threat environment, susceptibility risk depends upon factors, such as radar wavelength (gain pattern for the radar antenna, S/N ratio for target detection) and radar cross section (RCS) (IR signature). Being aware of the kill type, either a mission (mission abort) kill or system (quick attrition) kill, the critical components (CC) and their kill modes are identified.

Susceptibility $P_H$is estimated through simulation, while component vulnerabilities can be calculated, through fault tree analysis (FTA) and failure mode and effects analysis (FMEA) techniques, as in safety assessment techniques. For a component i, vulnerability $P_i(k|h)$ is defined

$$P_i(k|h) = A_v/A_p \tag{8}$$

where A_v is the vulnerable area of the component, and A_p is the component presented area. As the same calculation is executed for each critical component at several vulnerable areas of the aircraft, it is possible to draw a planar map of the aircraft, that can denotes the impact of a hit at a certain area and is used to reveal the areas of high vulnerability. To obtain such diagram, a Monte Carlo type of experiment is necessary. An example of a hit plot is shown in Figure 67

Vulnerability estimations are represented within the weapon envelope, depending on aircraft location (altitude and distance from the launch pad), as well as speed. For a naval combatant-fighter aircraft encounter, the weapon envelope looks like the one in Figure 68.

Figure 66: List of terminal effects (component kill modes) [16]

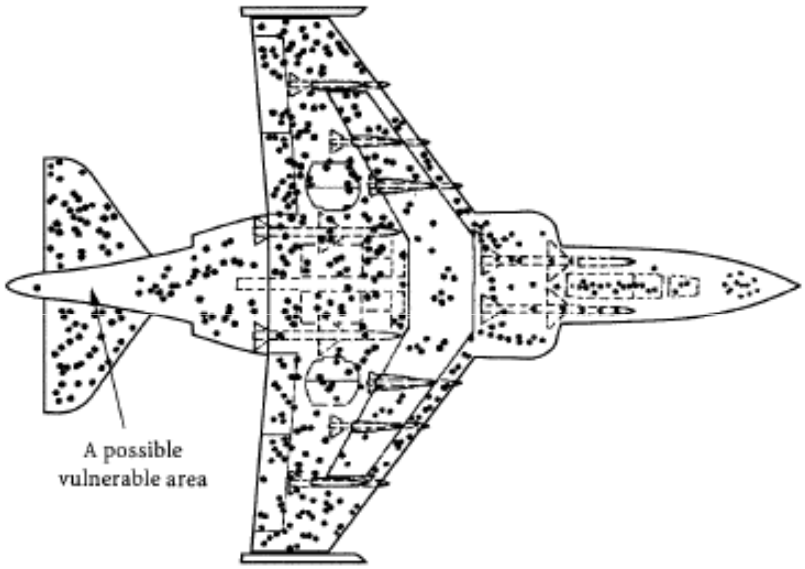


Figure 67: Hit plot for aircraft vulnerability assessment [16]

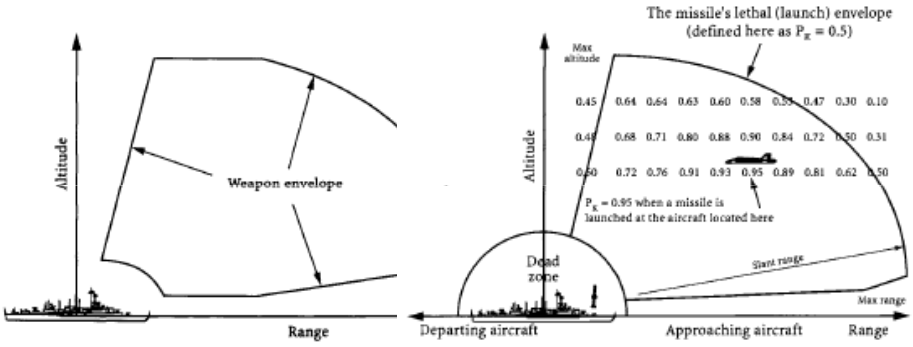


Figure 68: Weapon envelope for direct missile hit [16]

Figure 69: The Kill Chain [16]

For the case that the threat manifests itself through detonation of a warhead, estimation of vulnerability could be based on the use of a *kill function* $P_{K|F}$. The kill function is the probability density function (PDF) of the extension of the lethal area that is formed around the warhead, due to the impact of its detonation. When vulnerabilities are estimated for all critical components of the vehicle, the total vulnerable area of all components is obtained:

$$A_V = \sum A_v \tag{9}$$

and the total vulnerability for the vehicle/system is given by:

$$P(K|H) = A_V/A_P \tag{10}$$

where A_V is the vulnerable area of all components, A_P is the aircraft presented area.

For total survivability assessment, a single (or multiple) full scale mission scenario must be constructed and be broken down into mission segments. Each mission segment can be represented by a sequence of events, essentially describing a one-to-one scenario of an encounter between the system and the threat. To represent this sequence, a "kill chain" graph is used [16], as shown in Figure 69.

There is an unlimited range of possible formulations of the survivability equation. A step-by-step description of an event sequence is necessary for updating the survivability equation. With the kill chain, one can identify the key probability metrics (mostly conditional probabilities) and reformulate the survivability equation as follows

$$P_S = 1 - (P_H \cdot P_A \cdot P_{D/A} \cdot P_{L/D} \cdot P_{I/L} \cdot P_{H/I} \cdot P_{K/H}) \tag{11}$$

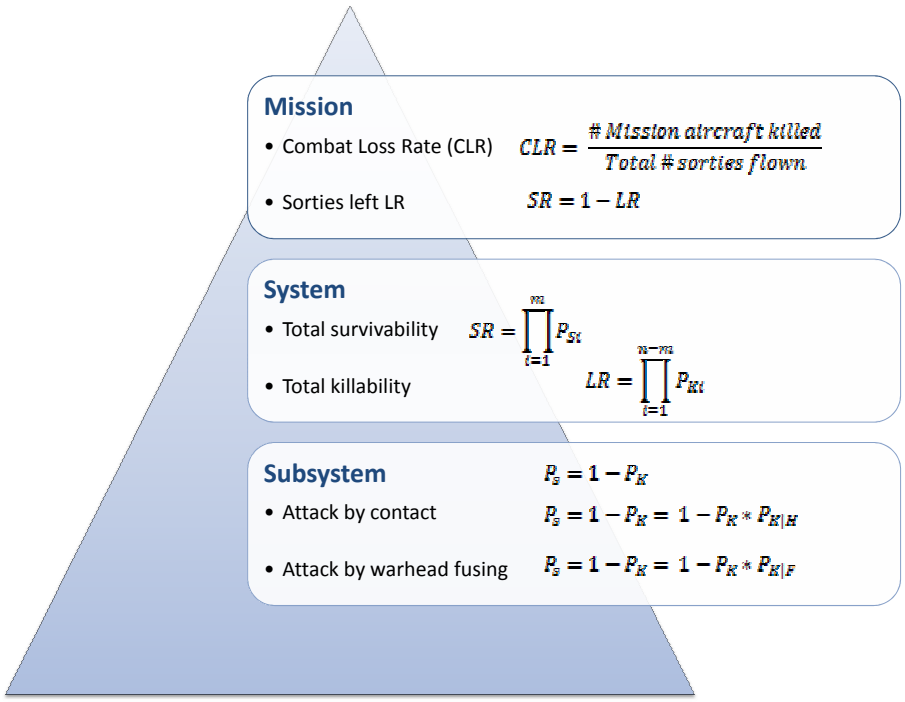


Figure 70: Engagement levels for total survivability assessment [16]

A kill chain based scenario can be thoroughly developed through a tree diagram and applied in all four engagement levels, component, system, mission or campaign level. It forms the basis of survivability assessment and the required probability calculations. An example of what calculations are performed at each level is shown in Figure 70.

3.2.1.2 SURVICE Survivability Assessment

The SURVICE company has suggested a survivability assessment method for Unmanned Aerial Vehicles (UAVs) [228]. While this method appears not be much different than the proposed approach by Ball, it does demonstrate how Ball's theoretical framework has been applied on a practical application. SURVICE breaks down survivability into four contributing factors, namely battlefield tactics, policy, mission planning and usage of weapons.

A mission scenario must be formulated and a kill chain representation describes the intermittent events from threat detection to possible system or mission kill. For

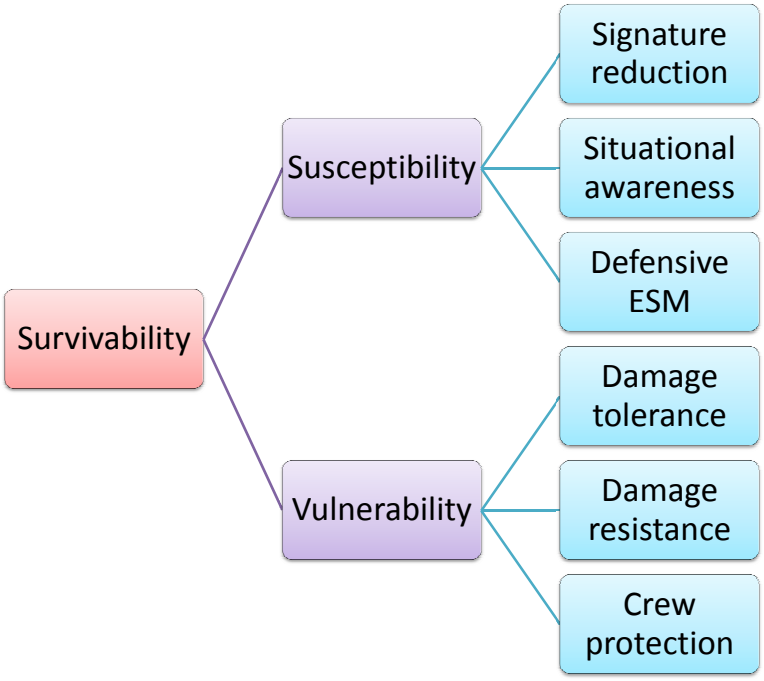


Figure 71: SURVICE survivability breakdown [228]

a UAV case, the kill chain contains the following sequence of events: Engagement-Acquisition-Track-Launch-Intercept-Fuzing-Hit-Kill. Probability of survival is calculated as in Ball's method. Finally, recommendations are given for enhancing survivability, either through susceptibility or vulnerability, as outlined in Figure 71.

3.2.1.3 Total Ship Survivability Assessment (TSSA)

The Total Ship Survivability Assessment (TSSA) method has been supported by NAVSEA for the Joint Command and Control Ship (JCC(X)), by building upon previous successful survivability systems engineering efforts. The TSSA emerged as part of the survivability requirements development, their impact on life-cycle cost, the concept of operations, and mission package [266]. It brings focus in quantifying operational effectiveness and provides realistic trade-offs by assessing cost and effectiveness impacts. It also recommends features for balancing survivability and effectiveness per unit cost. The process concentrates on platform level engagement

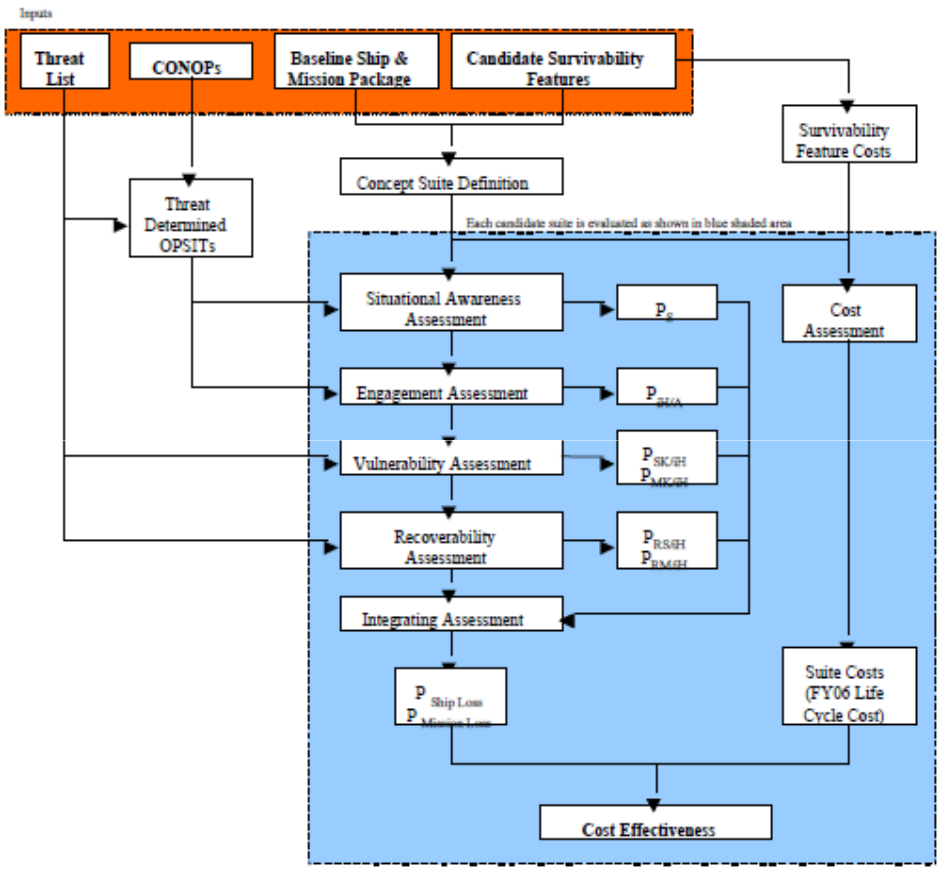


Figure 72: Total Ship Survivability Assessment Method (TSSA) [266]

analysis, thus excluding campaign and mission level assessments, and is represented in Figure 72.

To initiate survivability trade-offs for this study, one must identify possible combinations of threat weapons, accidents and associated operational situations. For each scenario, an event-based kill chain can be defined. The total probability of survival is estimated according to event-specific probabilities for a certain outcome to occur. For the JCC(X), a kill chain example is shown in Figure 73.

Based on Figure 73, the probability of mission survival is:

$$P(MissionLoss) = 1 - P_s \cdot P_{a|s} \cdot [1 - \sum (P_{th|a} \cdot P_{rs|th} \cdot (1 - P_{mk|th}) \cdot P_{rm|sh})] \quad (12)$$

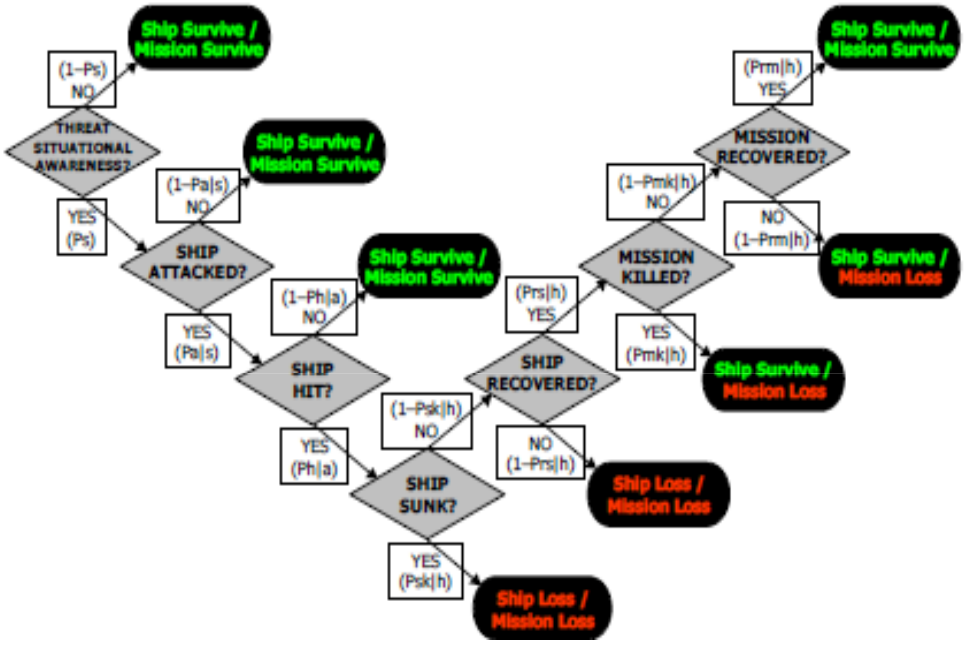


Figure 73: Kill chain for JCC(X) survivability assessment [266]

and for the system survival

$$P(ShipLoss) = 1 - P_s \cdot P_{a|s} \cdot [1 - \sum (P_{th|a} \cdot (1 - P_{sk|sh}) \cdot P_{rs|sh})] \qquad (13)$$

In the next step, two alternative design configurations are tested and assessed for survivability, one being the baseline configuration and the other an enhanced design for reduced susceptibility and vulnerability. For reduced susceptibility, situational awareness (SA) is enhanced with advanced threat detection technologies, as well as signature reduction strategies. Thus, probability of detection and engagement probability are reduced with the expected number of hits. For vulnerability reduction, strategies, such as hardening, separation and redundancy, reduces the likelihood of ship or mission loss, both given a certain number of hits. Last, overall recoverability consists of probability of ship recovery, given a number of hits, and the probability of mission recovery given the same number of hits. It reflects the ability to withstand secondary damage such as fire, smoke, and progressive flooding, or even more active recovery procedures, such as the ability to restore power, remove water, eject smoke

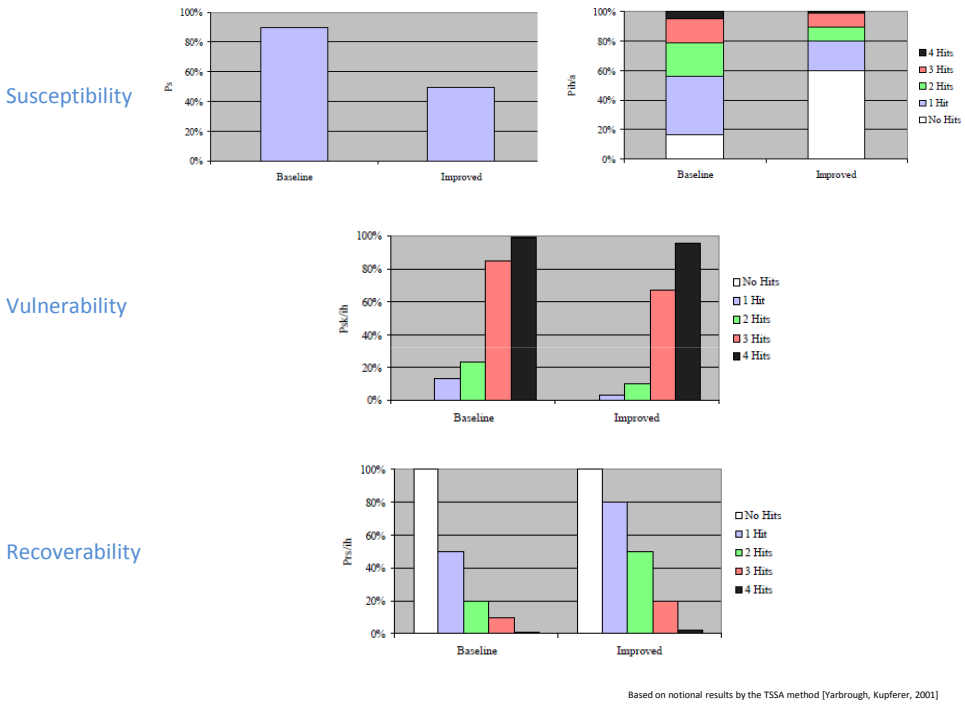


Figure 74: TSSA comparative results for different design configurations [266]

and restore mission capability. A representative way of summarizing and presenting the comparative results is illustrated in Figure 74.

Figure 75 displays the Pareto frontier on the cost-effectiveness relationship for ship survivability against procurement cost. To ensure that all designs are evaluated on an equal basis, survivability metrics were developed from the system analysis (SPs), then MOPs were combined to MOEs and plotted on a scatter plot for a large number of possible scenarios. The plot forms a Pareto curve, indicating the compromise between cost and survivability-based effectiveness.

In the final step, a decision must be made on what design configuration represents the optimal compromise among all other configurations. A histogram of total survivability along with the relative contributions is adequate in most cases for providing with an answer to this problem. The histogram in Figure 76, indicates for instance that concept C minimizes ship loss through some combination of susceptibility reduction, vulnerability reduction, and recoverability enhancement.

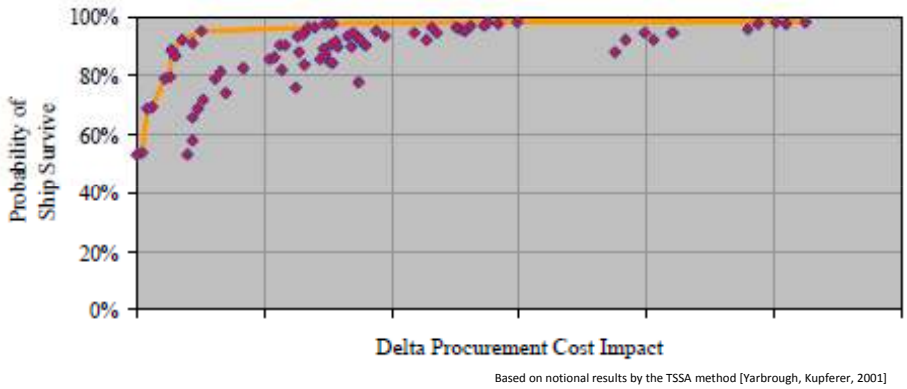


Figure 75: Cost-effectiveness Pareto frontier in TSSA [266]

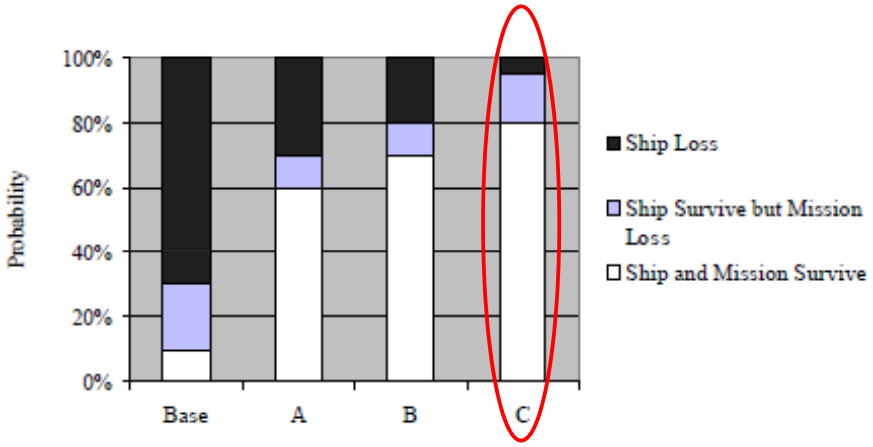


Figure 76: Histogram for optimal solution identification in TSSA [266]

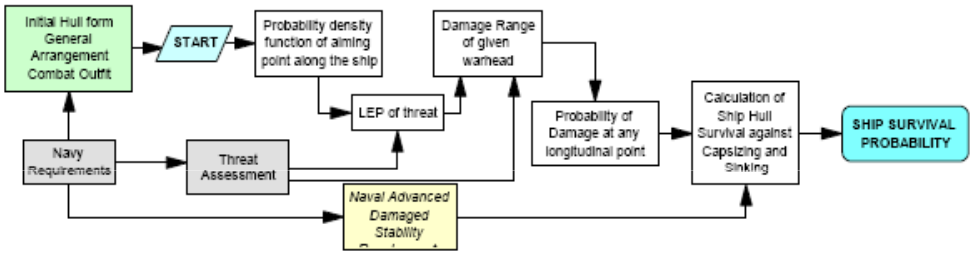


Figure 77: Ship survivability assessment for Ro-Ro class (IMO) [27]

3.2.1.4 Ship survivability assessment by IMO

The International Maritime Organization has recommended complete methods for conducting survivability assessment of Ro-Ro (ferry) passenger and merchant ships. The procedure is based on assessing the damage stability component of the vulnerability. In other words, it makes possible the assessment of damage cases, where multiple hits of nonadjacent compartments can occur. The assessment method is shown below in Figure 77.

Through the survivability assessment method, damage stability of the vessel becomes a substantial component of the design and allows for survivability to be a design attribute and not just a requirement or constraint. The integration with IMO's total ship design methodology approach shown in Figure 78.

3.2.1.5 Measure of Total Integrated System Survivability (MOTISS) by Alion

MOTISS is a system survivability evaluation tool, developed by Alion Technologies [8]. It integrates weapon effects and recovery analysis to assist in survivability-based design evaluation, requirements assessment, and resource allocation [8]. MOTISS also enables root-cause of failure determination, structural and network system evaluations, survivability design and option comparisons, vulnerability and recoverability evaluations, threat damage analysis (progressive fire, flooding, ballistic, jet, fragment and blast damage).

MOTISS is both an engineering process and a software application. As a process, it

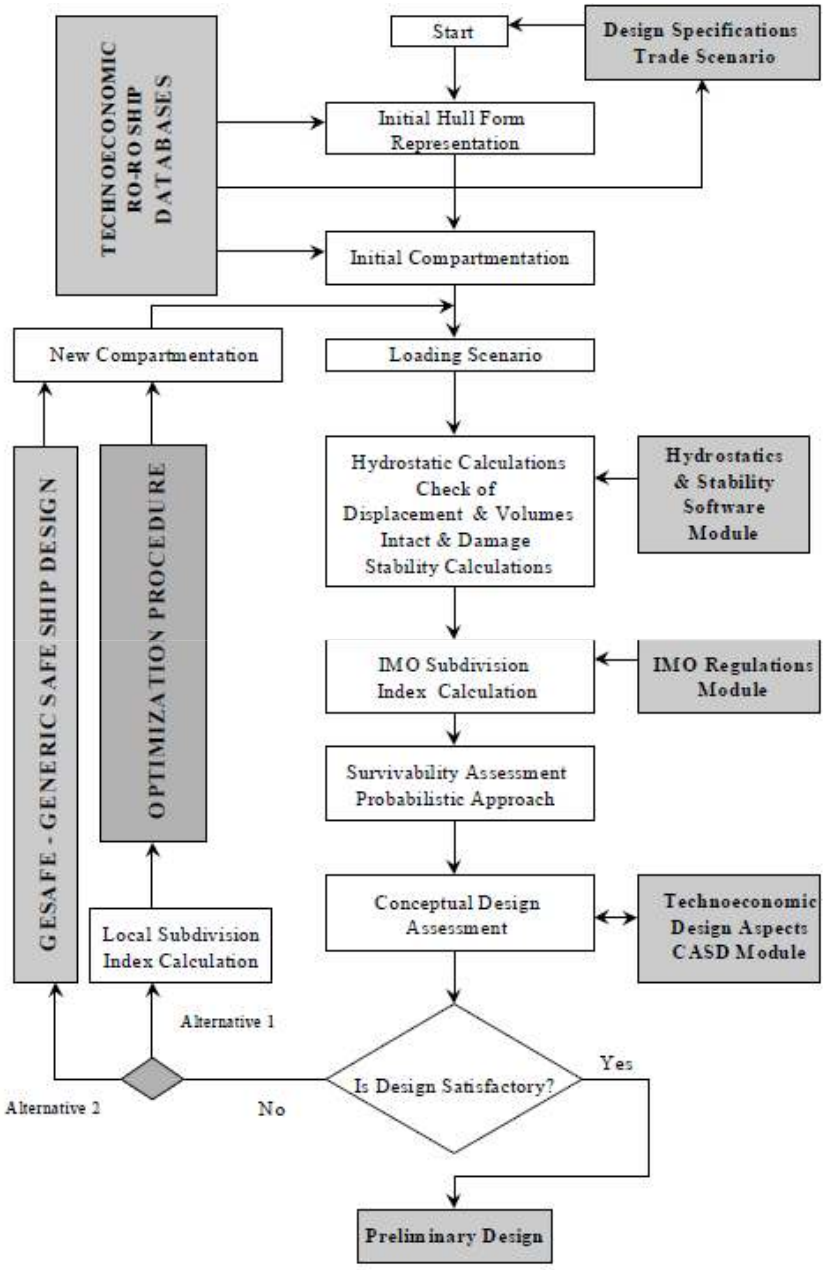


Figure 78: Ship survivability-based design according to SOLAS criteria for Ro-Ro class (IMO) [27]

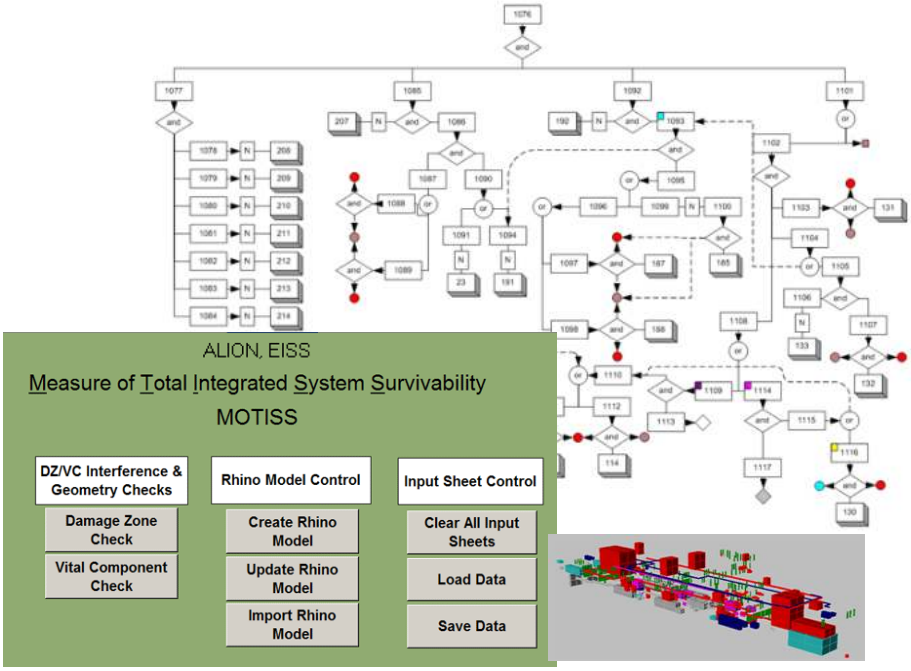


Figure 79: Alion's System Survivability design Process (MOTISS) [8]

can perform probabilistic survivability assessments for a system running on a mission with a one or more threats. It makes use of first principle physics, coupled with empirical data and tests to provide a rapid first order solution, considering multiple scenarios with varying threat and system parameters. An overview of the application is illustrated in Figure 79.

Another feature of MOTISS is that one can investigate and compare the effectiveness of two or more separate survivability enhancement design options, and determine which provides the best value for minimum cost. Furthermore, with MOTISS, the design can be parametrically altered, to find which design changes which have minimal cost or no cost, but enhance the ship's total survivability, and thus enhancing system effectiveness [8].

3.2.2 Evaluation of methods

In order to identify research opportunities and how SoA survivability assessment techniques could contribute to the development of a resilience assessment method,

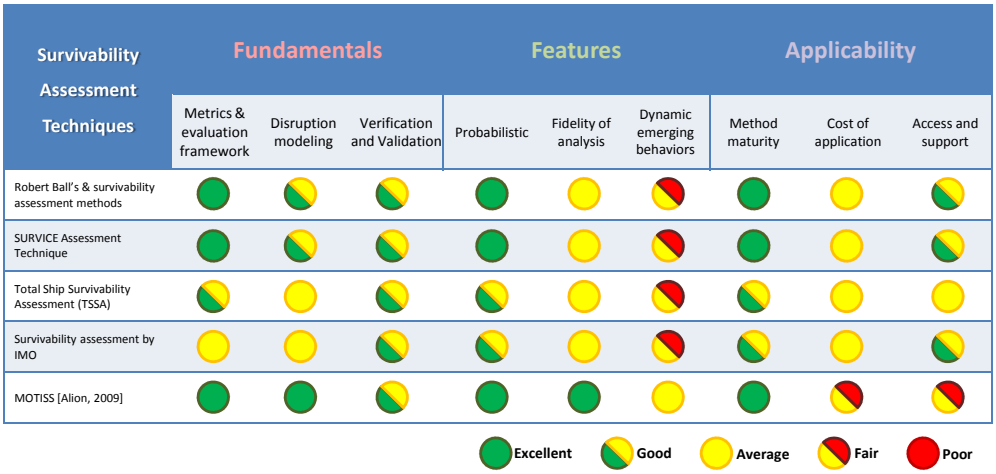


Figure 80: Evaluation of survivability assessment techniques

this section presents findings from the evaluation of the previously presented SoA techniques. The comparative qualitative evaluation results are shown in Figure 80. Regarding method fundamental attributes, most techniques are at the same capability level.

Given the fact that survivability definitions in engineering are very firm and transparent, it should come as no surprise that assessment techniques utilize metrics and calculations that are fairly standard. As the majority of methods are probabilistic, probability estimations rely on event sequences, in the form of the kill chain, for instance. Disruption modeling is based on scenarios with prescribed incidents, as in safety assessment. Dynamic transients and emerging effects cannot be captured, unless such capability is supported through a more advanced modeling and simulation environment. Verification and validation for these techniques has become possible, through testing in real world application. There is no global V&V guarantee however, since the techniques have been developed and tested in certain engineering application.

Observation 3.4: Survivability assessment techniques in engineering, rely on a quite

standard set of probabilistic metrics and calculations. Disruption modeling is prescribed through fixed scenarios. Techniques are developed and tested for particular applications, yet the latter should not prevent a technique to be upgraded for use in more engineering applications.

With risk and uncertainty recognized as prime factors of system survivability, assessment methods are probabilistic in nature. As part of monitoring fault and damage propagation, military survivability assessment is based on kill mode identification. Either historical information is required, or the use of physics-based simulations. The fidelity and capability of the simulation, as well as the detail at which the architecture topology has been captured, is critical for the ability of discovering transient and emerging behaviors. Most techniques though, employ basic kill mode identification enablers, resulting from fixed initial fault conditions, and assuming that disruptions are only binary.

Observation 3.5: Survivability assessment methods are probabilistic, and are based on fault scenarios. Transient and emerging (often unexpected), non-binary states are only captured with more advanced, dynamic physics-based models for kill mode identification.

Closing the evaluation with applicability of the assessment techniques, it appears that most of them are at a very satisfactory maturity level, given that they have been developed, tested and used by military authorities and the industry for several years. Cost of application is average for all three types of methods, however, execution may become more expensive, if advanced modeling and simulation approaches are commanded, as well as when they are applied on non-conventional concepts, with increased design uncertainty. Access and support depends on the engineering application, and the distribution rights by the releasing authorities. The MOTISS software package for instance, is a complete suite for survivability assessment, but it

is a tool that not all interested parties would have full access to, either due to cost or application restrictions.

Observation 3.6: Survivability assessment techniques are at a satisfying maturity level, and quite affordable, depending on the particular engineering application. The latter also determines access to the technique and general support towards it.

3.3 Resilience assessment methods

It has been argued that resilience engineering is still at its infancy stages, with researchers currently proposing scientific ideas, metrics and techniques for system resilience assessment. The majority of these efforts, have been leveraging similarities between the concept of resilience with system survivability, or system robustness, and often are augmentations of traditional survivability and quality assessment procedures.

3.3.1 Methods survey

Resilience engineering has been famously introduced to address ecological system stability. It is becoming relevant to other fields of science, such as economics and business, industrial systems and large scale organizations. At the same time, several traditional engineering disciplines are embracing the concept, with applications in materials, structures, infrastructures, architectures and other complex engineering systems. Resilience also applies on networks, such as supply chains, air transportation systems, and larger scale socio-ecological systems. Last, human behaviors and social interactions are addressed under the prism of psychological resilience.

Following the pattern of earlier SoA surveys on safety and survivability assessment techniques, a similar routine has been put in practice for discovery and identification of resilience assessment techniques. The investigation has returned a number of approaches, which refer to applications in the following engineering fields:

Techniques \ Applications	Systems Engineering	Civil Engineering	Materials	Network Systems	Resilient Controls
Resilience assessment framework [Madni & Jackson, 2009]	✓	✓		✓	
Dynamic survivability assessment SEARi [MIT, 2009]	✓	✓		✓	
Resilience assessment for materials [Mitchell, Boyd]		✓	✓		
Infrastructure and community resilience to disaster [Vugrin]	✓	✓		✓	
Networks (Air transportation / infrastructures)[Wang, Reed]	✓	✓		✓	✓

Figure 81: Origin and application of resilience assessment techniques

- Systems engineering
- Materials science
- Civil engineering and infrastructures
- Network systems

Figure 81 presents the selected, most prominent resilience assessment techniques, as they are mapped against the applications, or the engineering domain, based on which each technique has been demonstrated or developed.

Defining and assessing resilience in systems engineering, is the best proof regarding the recent scientific efforts for unifying resilience engineering in a framework that is suitable for all engineering applications. A serious step towards this direction has been taken by Madni and Jackson [146], who have redefined resilience, suggested metrics and compiled all contributions to propose a resilience assessment framework.

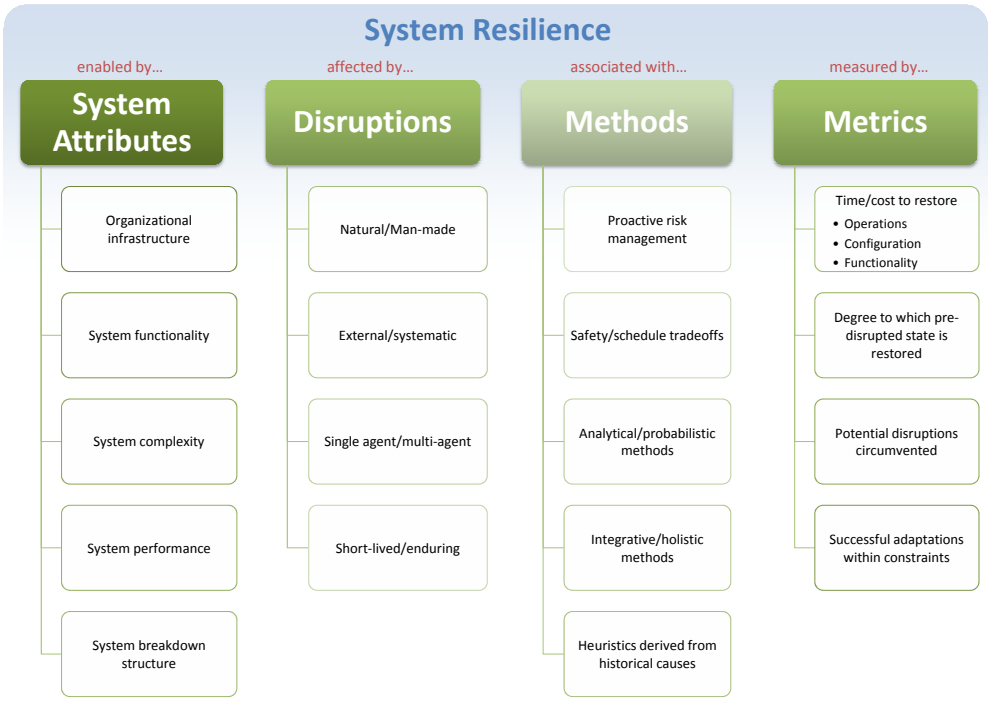


Figure 82: Resilience assessment framework by Madni and Jackson [146]

3.3.1.1 Resilience assessment framework by Madni and Jackson

Madni and Jackson describes resilience engineering as a discipline that is concerned with monitoring organizational decision making with explicit identification and monitoring of risks. According to their suggestions, a framework for resilience engineering is based on four key pillars: disruptions, system attributes, methods, and metrics, with Figure 82 presenting a concept breakdown of this framework.

Disruptions are characterized and classified as natural or man-made, external or systemic, single agent or multi-agent, and short-lived or enduring. The data of this classification should be stored and accessed through a reference database

System Attributes are the properties or characteristics of the system including organizational infrastructure, system functionality, system complexity, system performance and system breakdown structure. A disruption can impact one or more of these characteristics.

Methods of the framework contain a suite of traditional probabilistic risk assessments, operations-cost tradeoffs, integrative/holistic methods, history-derived heuristic database and proactive risk management. A key element to implement resilience is the effective production/safety tradeoffs. These will indicate the necessary compromise in production efficiency goals, in order to stay within the safe performance envelope. Having in mind that goals and environmental conditions constantly change, methods must be receiving feedback on the side effects of changes and organizational decisions on program and system risks.

Metrics are intended for monitoring risks arising from potential changes to daily practices and alerting about possible conflicts between operations and safety. As part of the prognostic nature of resilience, appropriate system models are required, that by using the necessary metrics, one could explain how emerging mishaps and accidents can happen, instead of solely relying on history-based predictions through cause-effect chains. Resilience metrics also contribute in demonstrating the validity and usefulness of each resilience attribute. For the reference, as part of their conceptual framework for system resilience, Madni and Jackson [146] have proposed the following generic types of metrics:

- Time & cost to restore operation.
- Time & cost to restore configuration.
- Time & cost to restore functionality and performance.
- Degree to which pre-disruption state has been restored.
- Potential disruptions avoided.
- Adaptability within time and cost constraints.

Hollnagel [111] also proposed a similar template. *Time scale* is a significant factor either for the disruption or its impact on system recovery. *Buffering Capacity* is a

general estimate for system robustness, namely its ability to withstand the change it is experiencing. *Self-restructuring capability* is related to the ability to recover from the occurred change. The last of four components is the system or subsystem *adaptation* as an aggregate estimate of the system's total response to the disruption.

3.3.1.2 Survivability assessment framework by SEARi(MIT)

Richards et al. at MIT's Systems Engineering Advancement Research Initiative (SEARi) have suggested metrics for survivability assessment of aerospace/mechanical systems, yet this approach was partially inspired by resilience engineering principles and the demonstrating application involved satellites and other space vehicles. The main objective is to incorporate survivability-based design into a generalized systems engineering approach for the design and acquisition of resilient and mission effective systems.

SEARi [155] has asserted that "non-traditional design criteria such as flexibility, robustness, survivability and others (referred to as the "ilities") are increasingly recognized as critical system properties for the success of aerospace programs". Such criteria are not always well-defined nor easily evaluated in isolation. In response to the need for a holistic framework with these non-traditional system design properties, McManus et al. have proposed a framework [155] that can be used to systematically incorporate "-ilities" into conceptual design and tradespace studies. The framework is based on a design space definition that allows for describing ilities in terms of changes in three dimensions. These consist of changes in the context (environmental condition), changes in the needs (stakeholder requirements) and changes in the system itself (physical system form).

The "-ilities" are the medium, through which dynamical system change is propagated in the 3-D design space. This results in a dynamic design space, unlike the 2-D static design space, which one would be working with, in a traditional design space

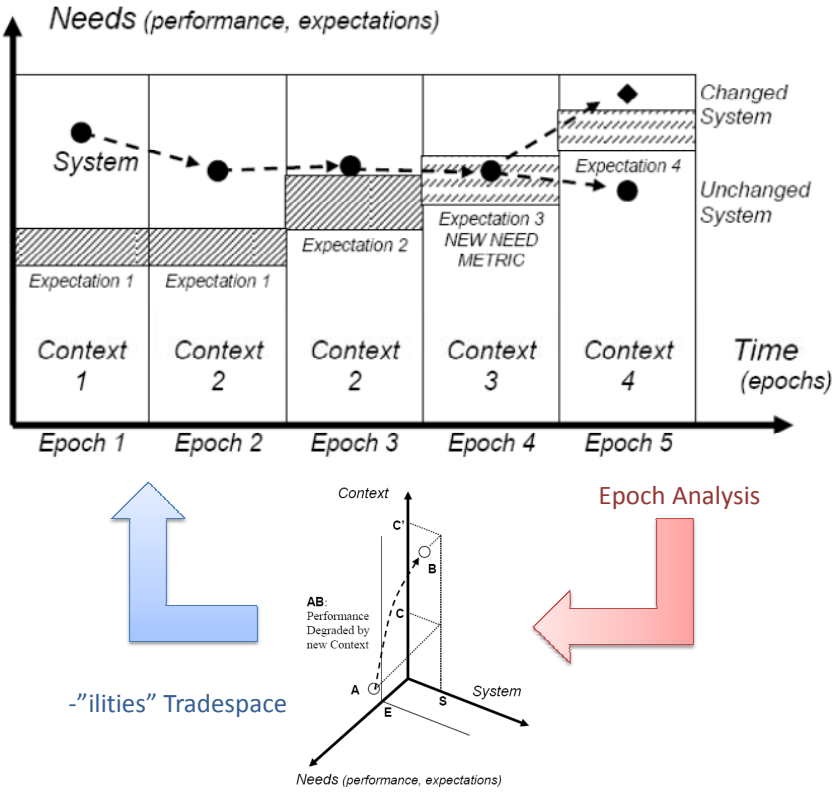


Figure 83: Epoch analysis and the "-ilities" tradespace representation [155]

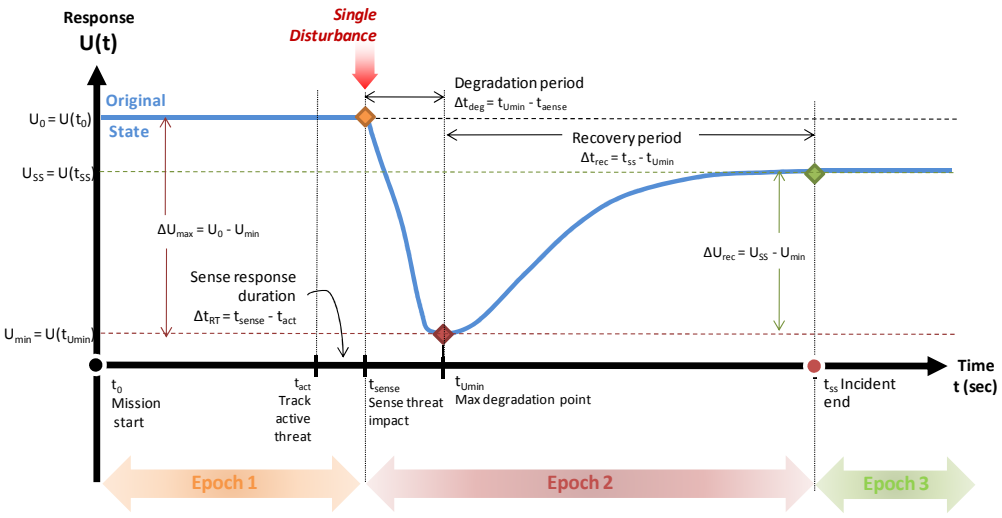


Figure 84: Dynamic system degradation and recovery

exploration study. Aside from the 3-D tradespace exploration, the discrete nature of the mission events that a system is experiencing, will have to be translated to continuous representation of dynamical changes. The *Epoch/era Analysis* links multiple discrete tradespace studies with time [155], with an example case study shown in Figure 83.

For initiating the epoch analysis, which would allow for the tradespace exploration, certain measures are necessary, regarding the system's dynamic performance response. Having defined the system's essential functions that represent value delivery and mission effectiveness, the system's dynamic behavior is typically described as in Figure 84. With an epoch defined as a time period with a fixed content, implying static constraints, design concepts, available technologies and attributes [198], the epoch analysis would return a chart of a standard format on the system's response under certain disruptions or performance degradations [190].

With the information of Figure 84 as the source, survivability estimations are guided by two major system objectives. First, utility loss must be minimized, while it must be also ensured that critical utility thresholds are met. Two metrics have been proposed metrics for total survivability assessment and these are:

- Time-weighted average performance degradation $\bar{U_L}$ and is the difference between initial utility value U_0 and the time weighted average utility $\bar{U_T}$ that is given by Equation 14:

$$\bar{U_T} = \frac{1}{T} \int U(t)dt \tag{14}$$

- Threshold availability A_T that is defined as:

$$\bar{A_T} = \frac{TAT}{T} \tag{15}$$

where TAT is the average time above threshold and is the percentage of time above a given threshold:

$$\bar{A_T} = \frac{t_{aboveThreshold}}{t_{total}} \tag{16}$$

3.3.1.3 Resilience assessment for materials

Compared to other engineering applications, the definition for materials resilience is specific. Assuming a fully elastic body, the work done in deforming an elastic body is stored up as elastic energy, which may be recovered as mechanical work when the load is removed. This elastic energy is called the *resilience* of the material [29]. Other equivalent definitions describe material resilience as "the ability of a material to absorb energy when deformed elastically and to return it when unloaded" [161] or the "extent to which energy may be stored in by elastic deformation".

If the stress on the body does not exceed the elastic limit, practically all the work which is put into it is recovered. If it goes beyond the elastic limit, part of the work is lost. The work expanded in deforming a unit volume of the material to the elastic limit, is called the *modulus of resilience* of the material. The latter is the elastic potential energy per unit volume, when the material is stressed to the elastic limit. It is a measure of the amount of energy which may be stored in a given material and recovered as mechanical work without loss. If a cubic inch of material is subjected to unit stress σ, the deformation is σ/E and the average force is $\sigma/2$, when the total

work is expressed as

$$U_p = (\sigma/E) \cdot (\sigma/2) = (\sigma^2)/2E \tag{17}$$

Equation 17 holds when σ is below the elastic limit. When σ is the unit stress at the elastic limit, namely $\sigma = \sigma_{yield}$, Equation 18 is the modulus of resilience.

$$U_{res} = (\sigma^2_{yield})/2E \tag{18}$$

As an illustrating example, consider a rod that is elongated, with x represent the total elongation in the rod of length l and unit cross section, and with dx representing an infinitesimal increment. When the elongation is x the unit elongation is x/l and the unit stress is $E \cdot x/l$. For the infinitesimal elongation dx, the unit work done on the rod is

$$dW = (E \cdot x/l) \cdot dx \tag{19}$$

Then, the total work for initial x_1 and final elongation x_2 respectively is:

$$W = \int_{x_1}^{x_2} (Ex/l) \cdot dx = (E/2l) \cdot (x_2^2 - x_1^2) \tag{20}$$

Substituting for x_1 and x_2 Equation 21 becomes:

$$W = ((\sigma_2^2 - \sigma_1^2)/(2 \cdot E)) \cdot Volume \tag{21}$$

From a graphical standpoint, material resilience (or the modulus of resilience), is the area under the stress-strain curve up to the yield stress, as shown in Figure 85. As explained earlier, it is the strain energy per unit volume required to stress the material from zero stress to the yield stress [160].

On a more practical issue, material resilience can be assessed and compared for a wide variety of materials and is generally measured using a uniaxial stress. Resilience can vary depending on the direction of stress for anisotropic materials, thus for isotropic materials, properties are not affected by direction in these materials. Last, for non-linearly elastic materials, Equation 18 does not hold, and graphical

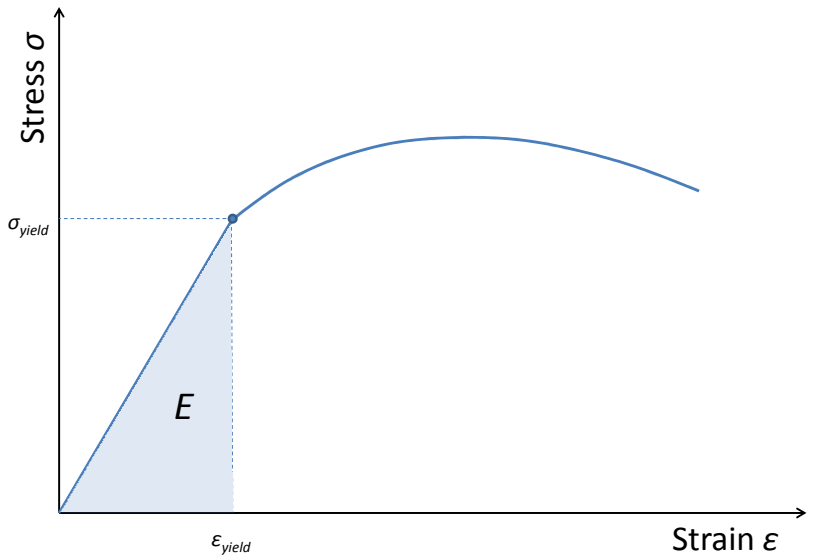


Figure 85: Graphical representation of material resilience [160]

methods are the only way to quantify resilience by computing the area underneath the stress-strain curve.

3.3.1.4 Resilience assessment for infrastructure and economic systems [251]

Resilience of infrastructures and socioeconomic systems has been emerging as one of the leading applications within the resilience engineering community. Vugrin et al. have suggested a framework for assessing resilience of a city infrastructure against disruptive events, such as flooding or earthquakes. The proposed resilience assessment framework consists of three core elements:

1. Definition of system resilience
2. Resilience cost measurement methodology (cost impact of system behavior to resilience).
3. Qualitative analysis component (resilience capacities and identification of enhancement features).

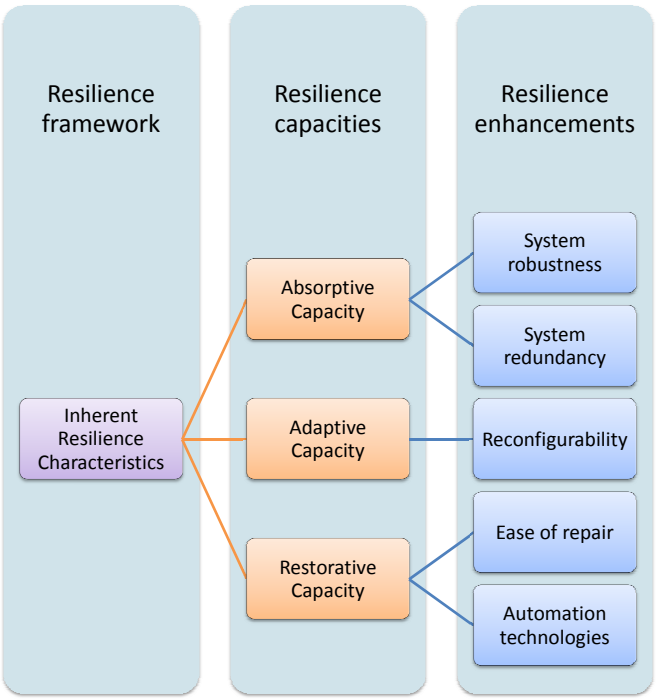


Figure 86: The three system capacities that affect resilience [251]

As part of the suggested definition of resilience, Vugrin et al. have been investigating the factors affecting resilience, which lead to a set of intrinsic resilience characteristics. These are expressed through the *resilience capacities*, which are the following:

- *Absorptive capacity* is the degree to which a system can automatically absorb the impacts of system perturbations and minimize consequences with little effort. It is an endogenous system feature and possible enhancements include system robustness (strength of individual internal system connections), and component redundancy(alternative system operation pathways).

- *Adaptive capacity* is the degree to which the system is capable of self-organization for recovery of system performance levels. It represents actions taken over time in response to the disruption, reflecting the dynamic ability of the system to change endogenously throughout the recovery period. Reconfigurability as the

extent to which the system possesses all necessary mechanisms and internal processes to change itself is both a characteristic and enhancement feature that is expected to improve adaptive capacity.

- *Restorative capacity* is the ability of a system to be repaired easily, with these repairs to be dynamic and performed by exogenous entities to the system. The goal is to allow the system to return close to its original structure. Ease of repair, either by design, or by the presence of a maintenance and support network is one possible way of enhancing restorative capacity. Other enhancements could include automation technologies to enhance restorative capacity, yet technology immaturity may impede the effectiveness of this approach.

The three system capacities as main contributions to system resilience, with associated enhancement features are shown in Figure 86.

Targeted system performance is a quantifiable measure of how the system performance should vary during and after disruptive events. For quantification of system resilience, the concept of *resilience cost* is introduced. Given that recovery is an inherent component of system resilience, Vugrin et. al suggest that recovery is a critical aspect of resilience that needs to be explicitly considered in measurements. Thus, resilience cost is linked to the expense of performing all necessary recovery efforts. The basis for this metric is founded on the premise that a system that moves quickly to the targeted system performance, but at a high total recovery effort, which may not be preferable to a slower, but less costly recovery. For the measurement of system resilience costs, the following factors are taken into account:

- Systemic impact, based on deviation from the targeted system performance levels.

- Total recovery effort, based on the duration of recovery.

- Recovery effort, based on costs and efforts required to change the system structure for targeted system performance level recovery.

It must be noted that taking just one factor into account, may not be adequate for full system recovery evaluation. While this still constitutes a partial assessment, it does not provide a transparent means for evaluating alternative recovery strategies, with different cost and required time, even with the same outcome regarding targeted performance. Figure 87 illustrates this point, with two systems that experience identical disruptions at precisely the same time. Both systems experience same decreases in system output, and both systems return to pre-disruption levels at precisely the same time. By only considering systemic impact, these two systems have identical resilience values, if resilience is the marked area that is bounded by the ideal and real performance degradation curves. If one also considers the recovery resources used for the same amount of necessary recovery, it appears that significantly more resources are expended for system 1 to return to original output levels. Thus, system 2 is considered to be more resilient because the recovery effort for identical system impacts had been less than system 1.

Regarding the quantification approach for resilience assessment, two key components of the resilience definition are taken into account, namely *systemic impact* and *total recovery effort*. Systemic impact is measured by evaluating the difference between a targeted system performance level and the actual system performance following the disruption, and is expressed by Equation 22:

$$SI = \int_{t_0}^{t_f} [TSP(t) - SP(t)]dt \tag{22}$$

Graphically, SI is quantified by calculating the area between the targeted system performance (TSP) and the actual system performance (SP) curves in Figure 88. Total recovery effort is measured by analyzing the amount of resources expended

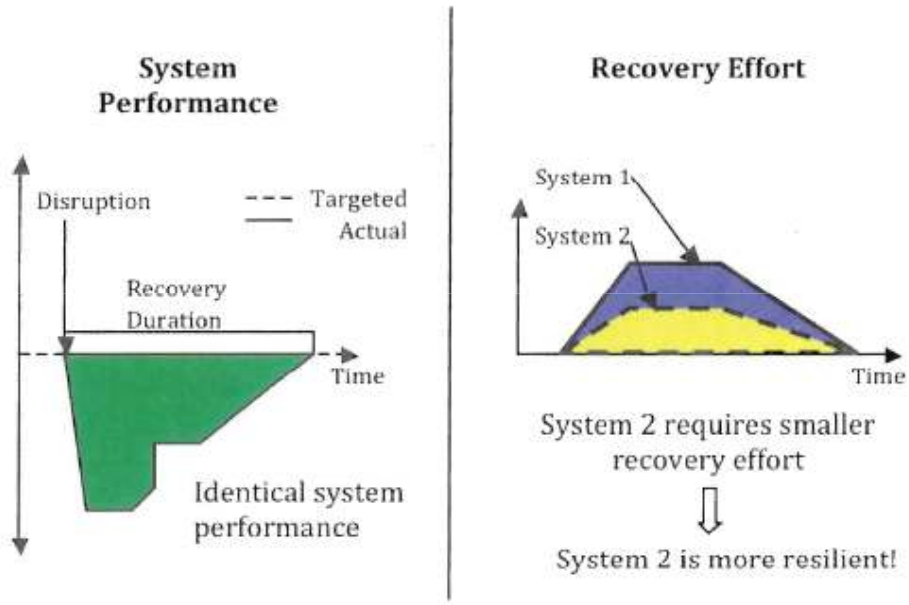


Figure 87: Impact of recovery mechanisms in resilience [251]

during the recovery process, namely as Equation 23 below:

$$SI = \int_{t_0}^{t_f} [RE(t)]dt \tag{23}$$

On the graph of Figure 88 TRE is represented by the area under the recovery effort (RE) curve. Higher level resilience calculations incorporate both of these quantities.

The next step is metric formulation to calculate system resilience costs by aggregating SI and TRE. Based on the hypothesis that systemic does implicitly depend on the selected recovery strategy, two resilience cost measurements were suggested: *Optimal resilience costs* OR are the system resilience costs against a particular disruption d, with the optimal recovery strategy (minimum combination of systemic impact and total recovery effort) and is described by Equation 24:

$$OR(d) = min_{RE} \frac{\int_{t_0}^{t_f} [TSP(t) - SP(t,d)]dt + \alpha \int_{t_0}^{t_f} [RE(t,d)]dt}{\int_{t_0}^{t_f} |TSP(t)|\, dt} \tag{24}$$

which returns:

$$OR(d) = min_{RE} \frac{SI(t,d) + \alpha TRE(t,d)}{\int_{t_0}^{t_f} |TSP(t)|\, dt} \tag{25}$$

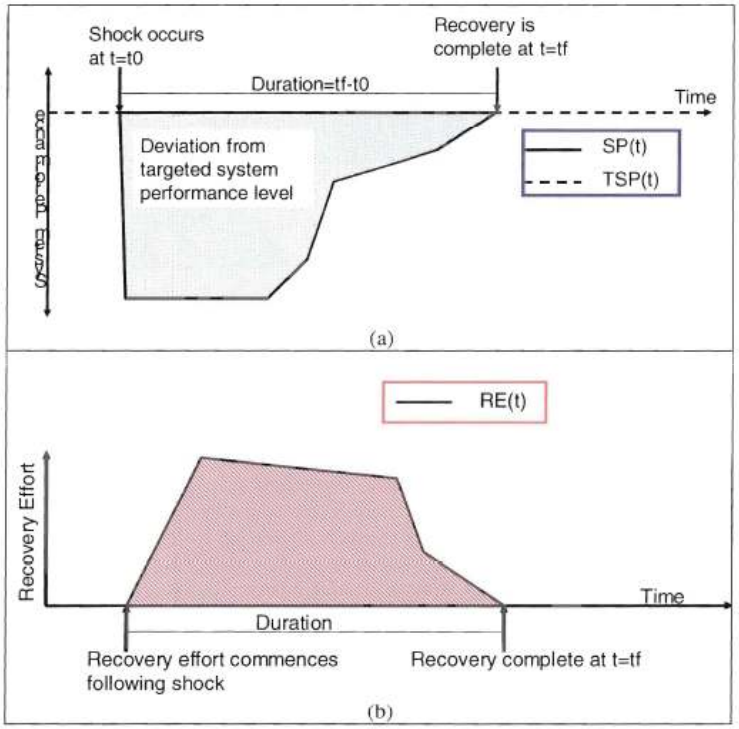


Figure 88: Visual representations of SP, TSP and TRE [251]

Recovery-dependent resilience costs RDR are the resilience costs of a system to a particular disruption d, with a particular recovery strategy RE and is described by Equation 26:

$$RDR(d, RE) = \frac{\int_{t_0}^{t_f} [TSP(t) - SP(t, d)]dt + \alpha \int_{t_0}^{t_f} [RE(t, d)]dt}{\int_{t_0}^{t_f} |TSP(t)|\, dt} \tag{26}$$

that is equivalent to:

$$RDR(d, RE) = \frac{SI(t, d, RE) + \alpha TRE(t, d, TRE)}{\int_{t_0}^{t_f} |TSP(t)|\, dt} \tag{27}$$

Both OR and RDR costs are normalized *linear combinations* of SI and TRE. Parameter α is a non-negative, non-dimensional weighting factor that allows assigning weighting factors to express the relative importance of SI and TRE (default equal weighting value is 1). It appears from Equations 25 and 27 that smaller RDR and OR costs indicate increasing resilience. The nature of the metrics allows for a series of tradeoff studies that one can perform. For instance, the following combinations of systems, disruptions and recovery strategies can be constructed;

- Resilience of *different* systems to the *same* disruption. The system that has lower resilience costs will be the more resilient system.

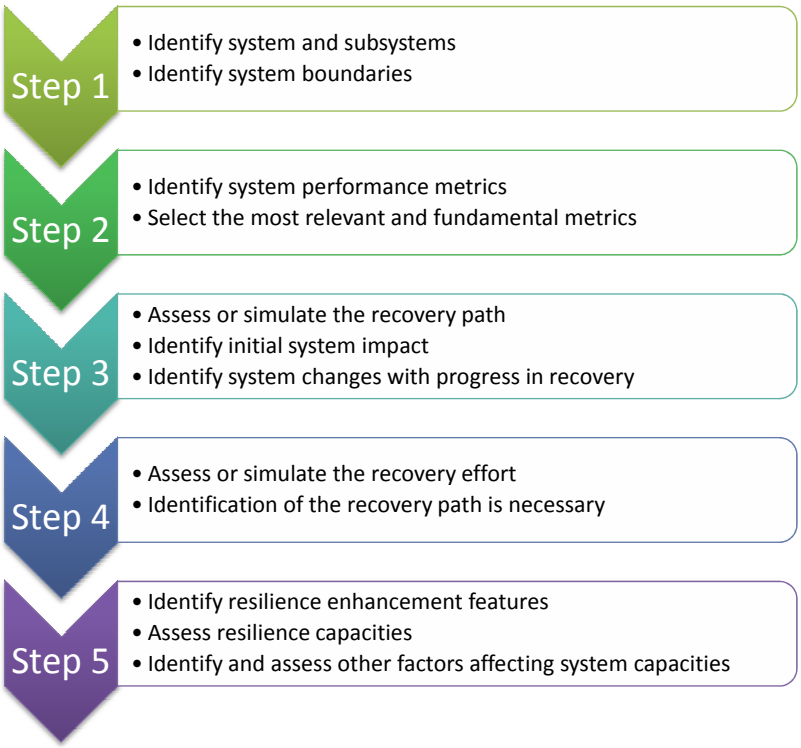
- Resilience of the *same* system to *different* disruption types. The system is more resilient to the disruption that results in smaller RDR and OR values.

- Resilience of the *same* system to the *same* disruption under *different* recovery strategies. Each different recovery strategy will result in different SI and TRE values. The recovery strategy that results in the smallest RDR values will maximize resilience for the system.

To illustrate the assessment method, Vugrin at al. have proposed a notional earthquake scenario. The objective of this resilience assessment was to provide a high-order, qualitative evaluation of the resilience of 18 regional infrastructure systems to an earthquake. An earthquake of magnitude 7.7 was assumed to occur, with several major natural gas transmission pipelines being ruptured as the immediate outcome. Additionally, cascading electric grid failure would likely occur, leading to a blackout on the region within 30 minutes of the event. With the method is explained in Figure 89, the evaluations were then gathered in a single resilience matrix, referring to two functions: emergency services and postal and shipping services. The matrix qualitatively describes with the letters H, M, or L (for high, medium, or low) the degree at which the three capacities of the infrastructure have performed, for the two critical functions.

3.3.1.5 Resilience assessment of organizations and infrastructures [54]

Except for complex systems, resilience also applies on other topological forms, such as organizations and larger scale infrastructures. From another perspective, an organization is a system, or a network of systems. Furthermore, a network can be a system or a network of organizations could be a large scale system. In the end, every system



Resiliency Matrix: Earthquake Scenario Analysis Example

System	Absorptive Capacity	Adaptive Capacity	Restorative Capacity
Emergency Services	L	M	L
Postal and Shipping	M	H	H

Figure 89: Resilience assessment method [251]

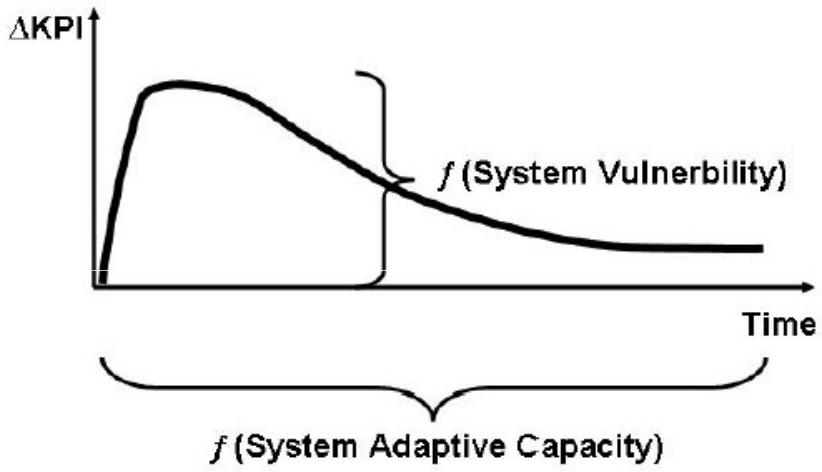


Figure 90: System KPIs as a function of adaptive capacity [54]

has properties that effectively represent its resilience to disruptions and unexpected factors.

With large scale systems organizations and networks, there is a great diversity of components, sub-networks and human working groups, regarding their individual local rules of operation and mission statement. To make an organization resilient, metrics and evaluations must translate and adjust to the mission of local sub-system entities within the organization.

Based on the organization's mission statement, a series of key performance indicators (KPIs) can be formulated, that are the measures by which the organization can track its performance against its stated objectives. Dalziell eta al. argue that the key performance indicators (KPIs) can be moved away from their desired levels will be a function of the system vulnerability. Organizational resilience is being brought by the adaptive capacity of the system, a function of which is the time it takes for the system KPIs to recover. The overall resilience of the system will be a function of the area under the curve, which is the total impact on KPIs over the response and recovery period, as demonstrated in Figure 90. An example of a full resilience assessment process for a disaster resilient community is given by Figure 91.

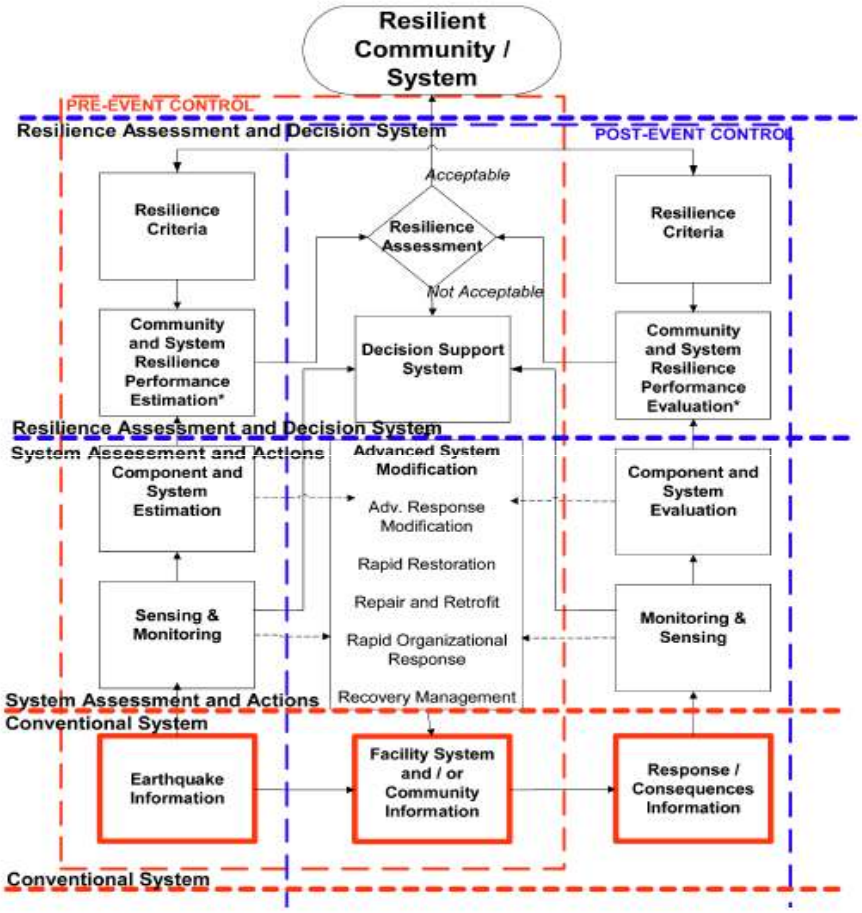


Figure 91: Resilience assessment for a resilient system community [54]

Quantification of resilience is an open subject for network-based applications in engineering as well. Some recent efforts have addressed the issue of a resilience metrics and assessment framework, Rosenkrantz et al., or Asha et al. to name a few. The latter authors have introduced the concept of *Structure-Based Resilience Metrics* to quantify the resilience of notes and edges in networks. On the application side, Wang et al. [256] have formulated a problem based on the air transportation system. Moreover, Kapur et al. have also looked at the resilience assessment problem, only using a networked infrastructure example to measure community resilience after major disasters [188].

3.3.1.6 Network resilience of the air transportation system

Wang et al. have proposed their own scheme, to make estimates of the network resilience of the air transportation system. It is a very large network that is highly interrelated to other networks, of smaller scale and of local deployment. A significant portion of the large network's support, originates from logistic networks on the ground, that guarantee flight safety, maintenance and other operating services. For the air transportation system, Wang et al. consider two possible views of the network. The macroscopic view includes the central warehouses or service centers connected as logistic networks to provide the maintenance or service to several airports in the network covered area. On the other hand, the microscopic view describes the area as just an airport. Several maintenance or service groups are serving various airplanes located on different parking aprons.

Wang et al have proposed a resilience evaluation approach, based on the redundancy and distribution of supply resources for logistic networks. Also, the multitude of supply and demand nodes is important, as well as the possible was through which these agents interact with each other. Graph theory is used for mathematical representations of network properties and metrics for resilience evaluation depend on these

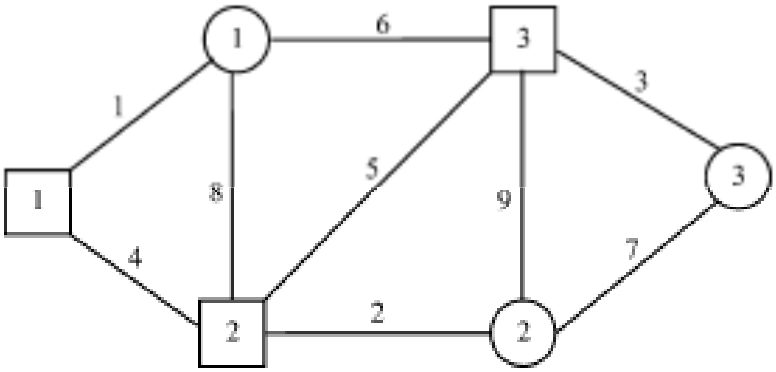


Figure 92: A bipartite undirected graph for network representation [256]

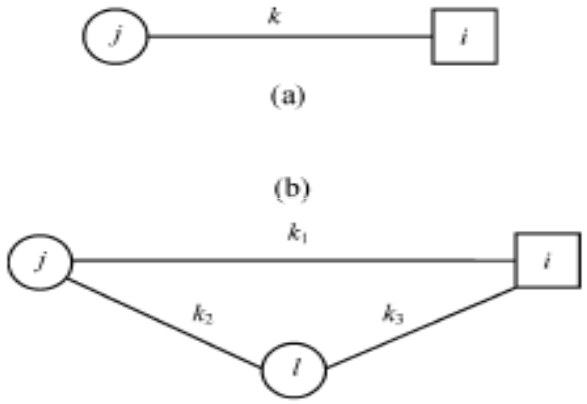


Figure 93: Combinations of demand supply nodes [256]

properties. A bipartite undirected graph for representing the network, is denoted as $G = \{D, S, E\}$, where D is the set of demand nodes, S is the set of supply nodes and E is the set of edges. Their corresponding number of members is n_1, n_2 and m respectively. An example of such graph is shown in Figure 92.

The next step is to define the values for demand and supply. For the n_1 demand nodes, demand of node i is d_i and is the requirement rate at unit time. For the n_2 supply nodes, available supply for node j is s_j and is the supply capacity at unit time. For the supply nodes j, reliability of supply is p_j. For an edge k, the flow capacity of the edge c_k is defined, along with the reliability q_k of the same edge. It is possible to have a number of supply-demand node combinations. In the case of a single supplier with a single delivery path, as shown in Figure 93-a, the resilience of the demand

node is defined as:

$$r_i = \frac{p_j \cdot q_j \cdot min(d_i, s_j, c_k)}{d_i} \tag{28}$$

In the case of multiple suppliers g, the resilience of the network is:

$$r_i = \frac{\sum_{j=1}^{g} p_j \cdot q_j \cdot min(d_i, s_j, c_j)}{d_i} \tag{29}$$

The total resilience of the network is defined as the weighted sum of all demand nodes

$$R = \sum_{i=1}^{n_1} w_i \cdot r_i \tag{30}$$

with the weights w_i defined as

$$w_i = \frac{d_i}{\sum_{i=1}^{n_1} d_i} \tag{31}$$

For a network with redundant supply nodes, the surplus supply will be:

$$\Delta = \sum_{j=1}^{n_2} s_j - \sum_{i=1}^{n_1} d_i \tag{32}$$

allowing for the definition of the redundancy coefficient u_i,

$$u_i = min\left\{\frac{\Delta}{d_i}, 1\right\} \tag{33}$$

which makes the revised resilience equation

$$R = \sum_{i=1}^{n_1} u_i \cdot w_i \cdot r_i \tag{34}$$

3.3.1.7 Resilient networked infrastructures

Reed and Kapur [188] have introduced a resilience assessment framework, that is applied on networked infrastructures. In fact, their application problem is the eleven-system interdependent infrastructure, containing the following entities:

1. Electric power delivery (distribution, transmission, and generation).

2. Telecommunications (cable, cellular, Internet, landlines, and media).

3. Transportation (air travel, roadways, fueling, mass transit, rail, water and port facilities).

4. Utilities (water supply, sewage treatment, sanitation, oil delivery and natural gas delivery).

5. Building support (HVAC, elevators, security and plumbing).

6. Business (computer systems, hotels, insurance, gaming, manufacturing, marine-maritime, mines, restaurants and retail).

7. Emergency Services (911, ambulance, fire, police and shelters).

8. Financial systems (ATM, banks, credit cards and stock exchange).

9. Food supply(distribution, storage, preparation, and production).

10. Government(offices and services).

11. Health care(hospitals and public health).

Reed at al. have proposed a resilience measure that combines two associated measures, *system fragility* and *quality*. As mentioned in earlier sections, fragility is a concept pertinent to resilience and has been extensively used by structural engineers to characterize the probability of damage given a level of hazard demand such as wind velocity or ground acceleration. Fragility is a means of representing the strength of a structure or a low rise building and a common way to represent this information is through the fragility curves.

In the context of the networked infrastructure, fragility of a line is the percentage of outages relative to the total number of customers residing within the boundaries of the infrastructure. Keeping in mind that engineers would use the term "inoperability" rather than "damage", fragility f_1 for a power line is defined by Equation 35.

$$f = P(inoperability|V^2) \tag{35}$$

where V is the appropriate wind speed parameter for the hurricane, while V^2 represents a dynamic wind pressure.

The earthquake engineering community is using another metric, the quality of an infrastructure. It has been derived by the MCEER [212] group and is intended to describe structural performance over time following earthquakes. Reed et al. have extended quality to include other possible inoperabilities due to several threats for disaster. Quality $Q(t)$ is given by Equation 36:

$$Q(t) = Q_\infty - (Q_\infty - Q_0)e^{-bt} \tag{36}$$

where Q_∞ is the capacity of the fully functioning structural system, Q_0 is the post-event capacity, and b is a parameter derived empirically from restoration data following the event. Parameter b is in other words a measure of the rapidity of the recovery. Also, $Q(t) = 1$ means the system is fully operable and when 0 means inoperable. Then resilience R of a system is defined as:

$$R = \frac{\int_{t_2}^{t_1} Q(t)dt}{(t_2 - t_1)} \tag{37}$$

and is visually represented by the area below the Q(t) curve on a Q-t plot. It has been also suggested that system robustness Rb is given as a function of quality $Q(t)$ as well

$$Rb = \frac{Q_\infty - Q_0}{/} Q_\infty \tag{38}$$

To calculate the total resilience for the infrastructure, resilience measures must be taken for all subsystems. Total system resilience is a function of the individual subsystem resilience measures:

$$R_{total} = g(R_1, R_2, ..., R_n) \tag{39}$$

with g being a function that reflects subsystem interdependence and connectivity. According to this particular formulation, it must be noted that the system resilience indirectly incorporates the rapidity and robustness parameters of the individual subsystems.

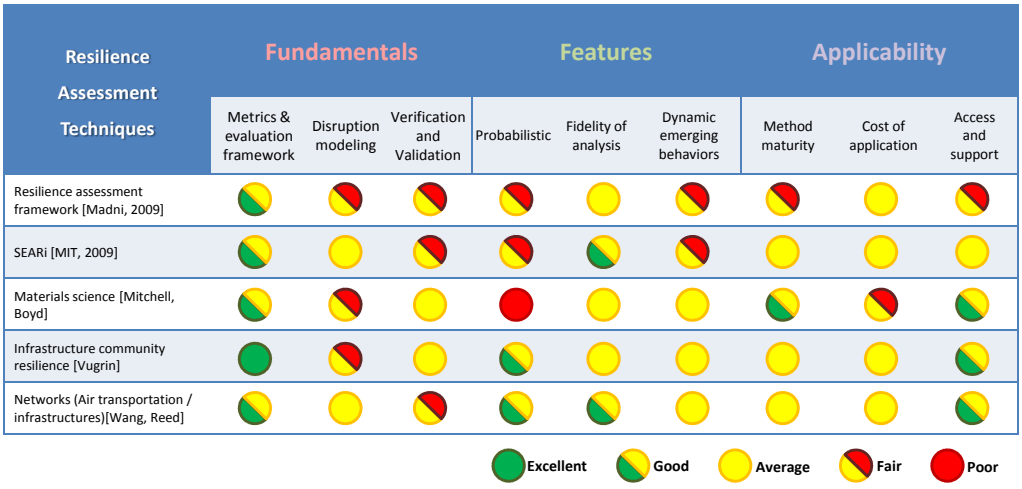


Figure 94: Evaluation of resilience assessment techniques

3.3.2 Evaluation of methods

Given that the development of a resilience assessment method remains the fundamental objective for this research, it is critical to evaluate the SoA in resilience assessment, and learn from these different approaches as well. The comparative qualitative evaluation results are shown in Figure 94. Starting from the fundamental characteristics, a different trend is observed, compared to earlier safety and survivability assessment techniques. Resilience assessment techniques are quantitative and utilize metrics and evaluation procedures that are in accordance to the attributes of resilience, as every technique is defining it.

Observation 3.7: Resilience assessment techniques are in principle quite similar to safety or survivability assessment, in terms of evaluation metrics, disruption modeling and scenario-based analysis. However, entities are suggesting their own application-specific definitions and evaluation approaches.

However, only basic disruption scenarios are taken into account, with fixed fault conditions, as in safety and survivability engineering tests.

Observation 3.7.1: Disruption modeling is currently done without much provision

on capturing combined, emerging and unexpected behaviors. It strongly relies on statistical information, or basic physics-based modeling and simulation.

With resilience being a very recent emerging engineering philosophy, most techniques have not been entirely verified and validated for their outcome reliability and real world relevance.

Observation 3.7.2: Due to the early stages of resilience engineering, resilience assessment techniques are not fully verified and validated in most engineering applications, especially for long term system performance.

There is no doubt that operational risk and environmental uncertainty are prime contributing factors to system resilience. While this has been acknowledged by the literature discussions, probabilistic calculations and uncertainty modeling have not been entirely integrated to the proposed techniques.

Observation 3.8: Despite the fact that uncertainty and risk have been addressed within the resilience concept, they have not been entirely implemented in current analysis techniques.

A key enabler in effectively addressing uncertainty, is the modeling and simulation environment, which is used for system analysis. One of the foundations of the resilience concept is the view of safety as a continuous and dynamic characteristic, which is dependent on dynamic system behavior. Equivalently, uncertainty and risk could be similarly observed. Under this premise, it is necessary to incorporate dynamic, physics-based models for capturing expected and unexpected emerging behaviors, especially for large scale, highly interrelated complex system architectures. Substantial, but minimal progress has been made towards this direction, not much on the physics-based modeling, rather than on capturing the interconnectivity effects, through network theory and graph modeling [256]

Observation 3.8.1: To successfully address uncertainty and risk, system analysis should be based on dynamic, physics-based models for capturing expected and unexpected emerging behaviors, especially for large scale, highly interrelated complex system architectures.

Following earlier observations, except for active developments in evaluation metric formulations, other aspects of resilience assessment techniques lie on a low maturity level. More time must be allowed for independent research efforts on different engineering applications, for reaching a point, where more capable simulation environments become available, as well as more sophisticated disruption modeling techniques.

Observation 3.9: Most techniques reside on a low maturity level, and further developments are necessary for properly addressing shortcomings in capturing uncertainty and the modeling approaches.

Cost of executing SoA techniques is fairly low, and is mainly driven by the analysis technique of choice. It is expected to increase with more sophisticated simulation tools, as well as disruption modeling techniques.

Observation 3.10: Cost of application is currently low and driven by the analysis and modeling technique of choice.

Access on technique documentation is open, however, for application-oriented and more dedicated implementation, it is expected that information may partially become proprietary.

3.4 Technical challenges and research opportunities

At this point, the overview of SoA approaches in safety management techniques has concluded. Chapter 2 brought focus on design methodologies, with safety, survivability or resilience as the main objectives. After this study, the objectives for this research have been repositioned and redirected towards the development of a

resilience assessment technique. Resilience assessment is a substantial enabler for resilience-based design space exploration and optimization. Following the evolving research focus, Chapter 3 has presented the literature search on resilience assessment techniques, for system safety, survivability and resilience. The literature search has revealed a diverse envelope of proposed approaches, extending to various scientific and engineering domains, and covering several engineering applications.

3.4.1 Summary of technical challenges in safety management SoA

Starting from safety assessment techniques, most limitations relate to fault and failure propagation modeling approaches, in conjunction to system functional and topological complexity. These are:

- No leverage of detailed function and topology information for predicting fault propagation.
- Static fault scenarios, formulated upon historical data does not allow for flexibility in capturing transient and emerging effects, that may lead to prediction of additional sources of fault and failure.
- Fault prediction assumes binary states, while it may be possible that there are more than two intermediate states of system degradation.
- Physics-based modeling for fault propagation prediction offers more accurate estimations, yet it is not always an affordable option, and a compromise between cost and accuracy must be considered.
- Reconfigurability and maintainability effects are not captured by the fault prediction modules.

In survivability assessment techniques, similar limitations have been identified. However, except for the fault propagation prediction modeling and complexity effects, additional ones are found:

- Except for fault propagation prediction, event development prediction (e.g. Kill Chain-based techniques) adds another layer of difficulty, which must be addressed by dynamic modeling and simulation.

- Kill mode identification (or catastrophic failure for non-military systems) becomes more challenging with increasing system complexity.

- Life expectancy or the time the system survives before it reaches kill mode/catastrophic failure, is a key survivability measure and dynamic simulations must accommodate for varying total operations duration.

- For complex networked systems, classic probabilistic calculations for survivability are insufficient. Advanced probabilistic or stochastic techniques must be investigated for capturing the increased complexity and dynamic transients.

- As in safety assessment, real time reconfigurability and maintainability must be incorporated in simulation environments.

Last, observations on resilience assessment techniques have returned another list of technical limitations that must be considered. As resilience assessment techniques are in principle quite similar to safety or survivability assessment, earlier limitations could still apply at this point. There is however an additional set of limitations, which originate from the philosophy of system resilience itself. These limitations are listed in following:

- Current resilience assessment techniques, are application specific.

- The identification of standard metrics, evaluation frameworks which do not rely on applications and adequately address the resilience of dynamical complex systems

- Even the most complete assessment techniques of current, would still require verification and validation for assuring the reliability of their estimations.
- Many technique proposals rely on non-probabilistic approaches, with risk and uncertainty not entirely addressed.
- Accident and fault propagation modeling must capture systemic events.
- Resilience assessment must be affordable enough to allow for parametric design and event space exploration.
- The technique must provide transparency in contributions to system resilience, whether it is due to architecture design effects, reconfigurability, adaptability and control architecture effects, maintainability or other.

For the purpose of method benchmarking, the literature investigation and technique evaluation has allowed for distinguishing a few of them. Probabilistic Risk Assessment (PRA) [220] is a good starting point, covering the basics in safety assessment, through risk identification and assessment. The survivability assessment technique by Dr. Ball, has been benchmarked for survivability assessment, and offers great insight for event formulation, experiments and probabilistic calculations for susceptibility and vulnerability, as well as how survivability is assessed and improved. Last, out the very few current attempt towards system resilience assessment techniques, the process by Vugrin et al. stands out, with an approach that is consistent with their resilience definition, with a quantitative evaluation framework and plenty of insight regarding the proposed directions, for improving and expanding the technique.

3.4.2 Research opportunities for the development of resilience assessment techniques

As a result of summarizing earlier observations on all assessment techniques, this section is discussing the corresponding research opportunities that are the key directions for the development of a resilience assessment method. These are organized in threads, which are the following:

- Theoretical framework formulation
- System and fault modeling
- Methods for assessment
- Implications in resilience-based design.
- Applications

The first thread involves the theoretical foundations for resilience assessment. It would refer to an ecosystem of fundamental definitions, necessary measurements, evaluation metrics (either on performance or more related to resilience) as well as statistical measures and correlations. Starting from definitions, these are the topics that must be addressed:

- Definition of resilience in engineering.
- Attributes and characteristics of resilient systems.
- Dependence of system resilience from the application.
- Association of resilience to other safety management concepts (safety, security, reliability, survivability).
- Association of resilience to robustness.

Remaining in the resilience framework, there are several opportunities in the quantitative aspect of the problem:

- Quantitative resilience estimations, either through physical metrics or objective functions.
- Independent variables, factors of resilience, along with sensitivities of resilience metrics to these factors.
- Quantification of constraints.
- Dynamic aspects of system resilience (transients, dynamic stability, time constants, etc.).

As the literature survey indicated, most attempts to address all previous research topics, have been specific to a focused application. Thus, metrics for system resilience have not been established to the point that can be applied as a standard for most applications. The lack of a standard analytical, quantitative and application-independent resilience assessment framework [146], has lead to an overarching research opportunity for the development of a unified, global resilience assessment approach.

As part of this overarching initiative, several opportunities arise on the modeling and simulation aspect of the resilience assessment problem. This thread however must be consistent with the vision of resilience engineering, allowing for the investigation of certain phenomena and resilience related behaviors, such as functional resonance, reconfigurability, life expectancy, maintainability and dynamic stability. The basic requirement, however, is the ability of the M&S environment to adequately predict fault propagation, system failures and accidents, based on dynamical system behavior. Historical data is expected to be inadequate, especially if revolutionary configurations are investigated, or unexpected phenomena are sampled. In short, the modeling aspect of resilience gives way to the following opportunities:

- Physics-based modeling for large scale complex systems.
- Dynamic system response analysis to expected or unexpected (emerging threats).
- Fault propagation modeling and prediction, system failure prediction, based on dynamic simulation results.
- Inclusion of reconfigurability and maintainability effects, for the implementation of truly recoverable systems.
- Modeling fidelity balancing (breadth & depth), according to resilience analysis requirements.

With the two first research threads on the theoretical aspect of resilience and with the required modeling approaches, most of the research efforts are concentrated on method development for assessing resilience. As part of formulating the building blocks for a complete resilience assessment technique, the following research opportunities arise:

- Scenario formulation and selection.
- Experimentation plans.
- Link equations between simulation data to resilience estimations.
- Screening tests for statistical significance of scenario effects (faults, degradations, failures, etc.)
- Effects of architecture and design characteristics on system resilience.
- Correlations of scenario effects to resilience estimates.
- Visual representations of resilience assessment.
- Method verification & validation.

- Cost of recovery and resilient response.

As the backbone for this dissertation, most of the upcoming research focus will be based on these research directions. These will be formally addressed through series of research questions, and the experimentation plan that is tailored for advancing the knowledge along these lines.

Resilience assessment however, is not where this research path is limited. The ultimate purpose of resilience assessment and evaluation techniques, is to support a resilience-based design methodology. Thus, assessment techniques must seamlessly integrate and be part of the larger design framework, and contribute towards design space exploration for large number of system configurations and evaluations against large number of scenarios for full uncertainty investigation. The upcoming research opportunities in support of resilient design space exploration are:

- Requirements analysis for resilient dynamical systems.
- Objective function and constraint formulation.
- Optimization algorithms for the design of resilient system architectures.
- Technology effects for improving resilience.
- Automation and control strategies.
- Optimization for reconfigurability and maintenance strategies.
- Compatibility of resilient system design solutions.
- Addressing "unexpected" uncertainty factors in the design process.

As stated in the introduction, before certain design oriented research tasks are reached, development and validation of resilience assessment techniques must first take place, in accordance to the scientific methods.

Assessment and design space exploration techniques are envisioned to be application and system independent. As this requirement would ensure the added value of the technique, it is not possible to ensure that this will be the case for all engineering application and all kinds of small/large scale dynamical systems. For the purpose of developing the technique, as well as demonstrating it with an application of an adequate scale, the appropriate baseline system configurations must be selected. To remain consistent with the original problem formulation and taking into account the modeling & simulation environment availability, the following options have been considered:

- Power generation and distribution systems.
- Chilled water systems.
- Network architectures.
- Large scale power grids.
- Civil infrastructures.

These options are considered for the demonstration of the technique. A smaller scale dynamical system configuration will be chosen as a *canonical* problem to assist in developing the technique. The criteria for canonical problem selection concentrate on scalability, transparency of transient and steady state behaviors, and overall simplicity, customization and portability. Last, similarities in form and dynamic behavior of the canonical problem to the larger scale demonstration configuration must be also apparent.

CHAPTER IV

RESEARCH AND EXPERIMENTATION PLANNING

In this chapter, research directions are being established, based on the technical challenges that have been identified and discussed in the previous sections. Chapter 4 facilitates the transition from research need identification and background investigation, towards the experimentation plan setup, for supporting the proposed approach in addressing the problem. In the following sections, the research questions along with the suggested hypotheses are presented, as well as the complete dissertation experimentation plan.

4.1 Formulation of the research questions

In accordance to the steps of the scientific method [151], the literature review has allowed for the identification of the fundamental directions for this research. Except for the research objectives in Chapters 1, 2 and 3, these directions are expressed through a set of *research questions*. They address phenomena, effects, and relationships of interest, which will guide the research contributions, for answering the research questions. Figure 95 describes the progression of the research objectives to the research questions.

Research question RQ1 is addressing the need for a generalized framework for system resilience assessment. The overarching goal is to provide and support a definition of resilience in engineering. Although this may not be possible within this iteration, it is expected for the proposed framework to be independent of the system application. Thus RQ1 is expressed as:

Research Question RQ1: How are resilient systems in engineering defined and

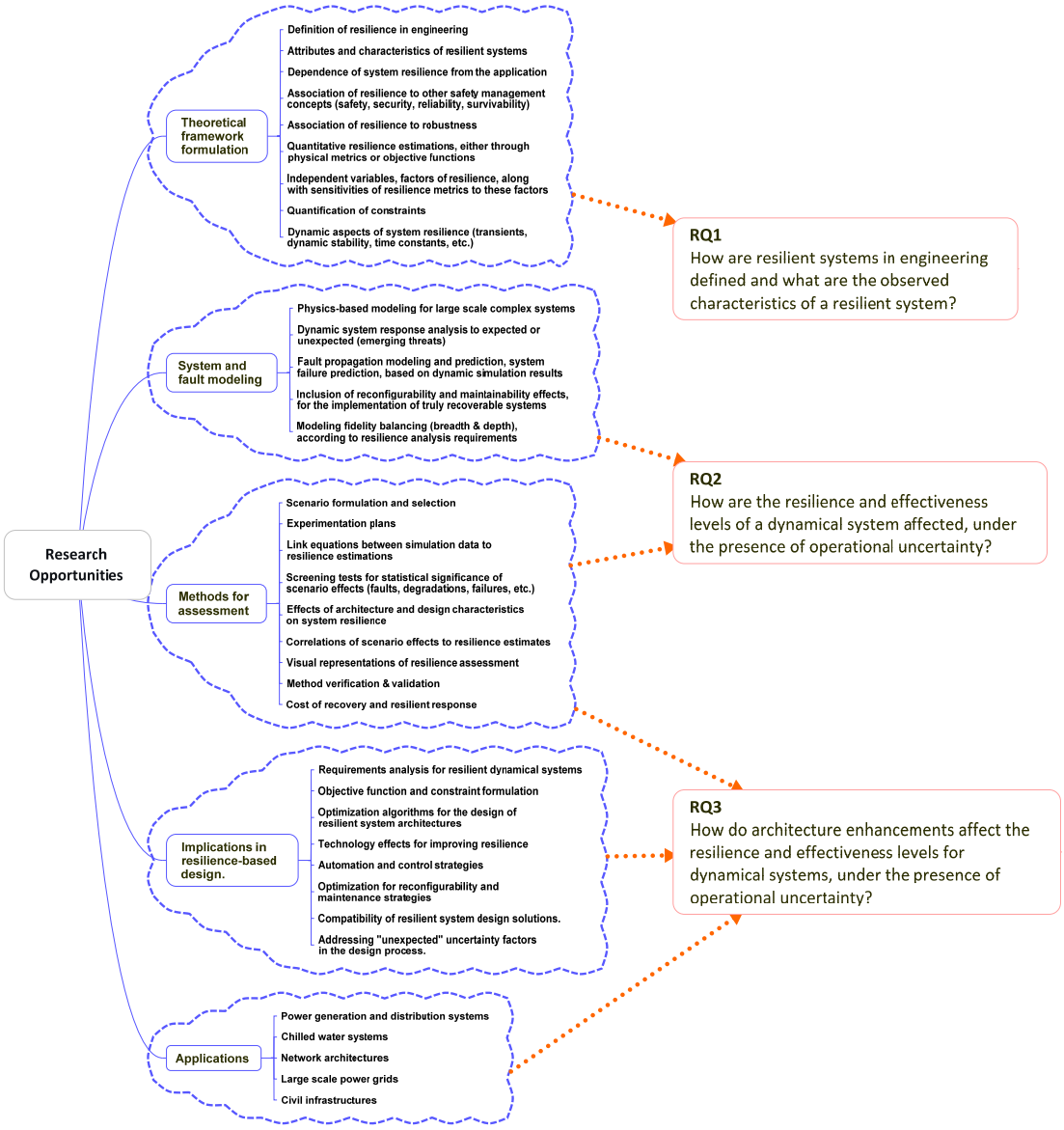


Figure 95: From objectives to research questions

what are the observed characteristics of a resilient system?

By linking RQ1 to the identified research opportunities at the end of Chapter 3, the intent is to investigate the built-in attributes and observed characteristics of resilient systems, as well as their association to safety management concepts (safety, security, reliability) and survivability, in particular. Clarification of similarities to system robustness is also a consideration.

With the introduction of the definition, attributes and observed characteristics for resilient dynamical systems, Research Question RQ2 leads the research efforts towards the formulation of a process for assessing dynamical system resilience, under the presence of uncertainty. It is expressed as follows:

Research Question RQ2: How are the resilience and effectiveness levels of a dynamical system affected, under the presence of operational uncertainty?

Besides being the basis for the development of the resilience assessment technique, other relevant issues are addressed by RQ2, such as the necessary experiments, input scenario formulation to capture operational uncertainty, screening tests for statistical significance of scenario effects (faults, degradations, failures, etc.), as well as method verification & validation.

Up to this point, RQ1 and RQ2 have been leading the development of a resilience assessment technique. The ultimate purpose of resilience assessment and evaluation techniques, is to ultimately support a resilience-based design methodology. Thus, assessment techniques must seamlessly integrate and be part of the larger design framework, and contribute towards design space exploration for large number of system configurations and evaluations against large number of scenarios for full uncertainty investigation.

Research Question RQ3: How do architecture enhancements affect the resilience and effectiveness levels for dynamical systems, under the presence of operational

uncertainty?

RQ3 concentrates on investigating options for improving system resilience. Among these options, resilience on certain levels of uncertainty may be improved with enhancing system reconfigurability, adaptability, or advanced architecture design approaches. The quantification of the impact for these solutions, is expected to support design exploration, constraint quantification, and the development of optimization algorithms for resilience as a design objective.

4.2 Hypothesis formulation and support

The research scope for this dissertation has been finalized under the three main research questions that were presented in the previous section. However, this scope is still quite large and volatile, in terms of possible approaches for addressing the research question. According to the scientific method, the research hypotheses introduce scientific evidence, and rigorous thinking, towards a suitable and adequate solution to the stated research problem. The hypotheses could be based on a hierarchy of assumptions, assertions and more fundamental hypotheses, responding to an equivalently hierarchical structure of research questions.

In terms of constructing a hypothesis, it could be formulated as a suggested explanation on given observations, knowledge from literature search, or it could be based on a working assumption that is bound to be tested, through proper experimentation. Hypothesis formulation is critical task, which sets the ground for the experimentation plan, as hypotheses must be testable, supportable and falsifiable [151]. Indeed, the falsifiability conditions determine the tests that must be planned for hypothesis testing. The following sections discuss the breakdown of the three main research questions, to a hierarchy that will allow for an effective hypothesis formulation, touching most of the different aspects of each research task. Corresponding to the main research questions, three main tasks have been introduced:

1. Theoretical framework for resilience assessment (RQ1).

2. Dynamical system resilience, under the presence of operational uncertainty (RQ2).

3. Adaptability and robustness tradeoffs in resilient systems (RQ3).

4.2.1 Theoretical framework for resilience assessment (RQ1)

As stated earlier, the goal for this research thread is to formulate the essential elements of the resilience framework. Besides a clear, universal and comprehensive definition for resilient dynamical systems, it is necessary to investigate other aspects, such as the attributes, and characteristics of resilience. Resilience characteristics, are the features that could be observed through testing and experimentation, and serve as a manifestation for the resilience levels of dynamical systems. Resilience attributes refer to intrinsic system capabilities, which allow for a system to be resilient. The attributes and characteristics are the basis for a framework, which will allow for quantitative resilience estimations. The framework is the backbone of the resilience assessment technique under development.

4.2.1.1 Observed characteristics of resilient systems

In order to better understand the characteristics of resilient system, a starting point is the exploration of the system's dynamic behavior and the discovery of certain trends, such as recoverability, mission and health level restoration, life expectancy and recoverability. RQ1.1 is setting this research direction and is expressed as:

Research Question RQ1.1: What are the observed characteristics of resilient systems?

The literature suggests that there is a great diversity in the types of dynamic system

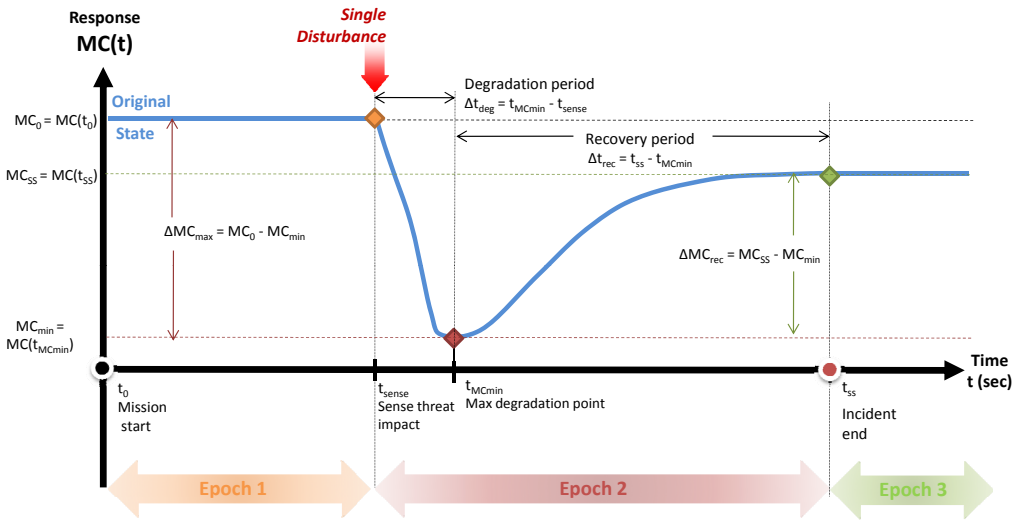


Figure 96: Typical restoration process after a single disturbance on a dynamical system

behavior, that different resilience frameworks are based upon, for their response analysis. Dynamic responses that are linked to resilience, such as system health degradation, or others that are associated to mission objectives, such as system performance ability, are some examples.

At this point, it is necessary to clarify the basic behavioral patterns of dynamical systems, before proceeding. In Figure 96, a typical response curve of a dynamical system's mission performance is presented. The system's response can be broken down into three phases, or *Epochs*. In Epoch 1, the system maintains its original performance state and health status, without experiencing any disruptions. At the end of phase 1, an unexpected disturbance, forces the system to degrade its performance, with possible adverse implications in its health. The system's performance degrades, yet it does reach a minimum point and then performance improves, as the system is heading for recovery. In Epoch 3, the system either fully or partially restores its mission performance ability.

As some of the literature work recommends, recoverability is a basic resilience characteristic, that is manifested through a dynamical system's response. There is

however no standard method for quantitative estimates of a system's ability to recover after a given disturbance. Understanding that the impact of resilience-based design solutions is a long term goal, RQ1.1.1 is introduced:

Research Question RQ1.1.1: How is it possible to quantify recoverability?

System recovery is a collective result of partial system efforts, towards restoring its health status and its mission performance ability. In other words, for complete recovery the system must:

- Recover performance
- Maintain/Restore mission performance ability
- Maintain/Restore system health (subsystem connectivity and integrity)

Based on the three recovery tasks, a set of corresponding quantitative estimations is introduced. It is also assumed that dynamic system performance is available, similar to that of Figure 96, and is representative of the system's Mission Capability $MC(t)$ time history. The performance minimum point is:

$$MC_{min} = min(MC(t)) \tag{40}$$

while the total degradation from the original performance point is:

$$\Delta MC_{deg} = MC_{min} - MC_0 \tag{41}$$

Based on the minimum performance point MC_{min}, one can solve for the time point $t_{MC_{min}}$, at which the minimum performance point occurs:

$$t_{MC_{min}} = t(MC_{min}) \tag{42}$$

which is the starting point for estimating the recovery time, until a steady state is reached. The minimum time required Δt_{rp} to reach a restoration steady state is the

time elapsed from the performance minimum $t_{MC_{min}}$ up to t_{ss} recovery:

$$\Delta t_{rp} = t_{ss} - t_{MC_{min}} \tag{43}$$

where t_{ss} is the time point, when steady state has been reached. At t_{ss}, the system has been restored at the value MC_{ss}, which is not necessarily the original value MC_{t_0} = MC_0. The restoration point offset from the original is:

$$\Delta MC_{rec} = MC_{ss} - MC_0 \tag{44}$$

The total recovery time Δt_{rt} is the total degradation time Δt_{deg} plus total recovery time Δt_{rp}

$$\Delta t_{rt} = \Delta t_{deg} + \Delta t_{rp} \tag{45}$$

Based on the restoration point offset, a metric equivalent to steady state offset can be defined as:

$$e_{ss} = |(\Delta MC_{rec})| = |(MC_{ss} - MC_0)| \tag{46}$$

However, the system might not be fully restored to its original value MC_0.

Another response of interest, is the *recovery rate* RR. The average recovery rate ARR at which the system's mission performance ability is restored is:

$$ARR = \Delta MC_{rec}/\Delta t_{rp} \tag{47}$$

namely the averaged time derivative of the mission performance value for the recovery phase.

Besides mission capability MC, the system is expected to maintain subsystem connectivity and integrity. As part of its ability to maintain its health, the SH_{ratio} ratio is defined, either for component or connectivity status.

$$SH_{ratio} = SH_{ss}/SH_0 \tag{48}$$

where, SH_{ss} and SH_0 are the health indicators for the steady and the original state, respectively. The health indicator SH is defined as the fraction of the number of

damaged/inoperable components over total initial number of components:

$$SH_{Damaged} = N_{Damaged}/N_{Total} \tag{49}$$

The purpose of the analytical formulation for dynamical system behavior analysis, is to further support resilience-based design methodologies and become one of the building blocks of the resilience assessment. As a response to RQ1.1.1, Proposition 1.1.1 reflects the need for the above dynamical system behavior analysis:

Proposition 1.1.1: Unless a threat is avoided and no performance degradation is observed, a resilient system's ability to recover its mission from a given performance degradation, is a measure of its recovery rate and time, and of the number of restored/replaced components, regarding its health levels.

Another observed characteristic of more resilient systems is their improved life expectancy and survivability, under the presence of external disturbances, in the form of faults or failures. Therefore, Research Question RQ1.1.2 brings attention on quantification methods for survivability:

Research Question RQ1.1.2: How is it possible to quantify survivability?

According to Ball's classic survivability formulation, survivability is defined as:

$$P_S = 1 - P_K \tag{50}$$

where, P_S is the probability of survival and P_K is the killability, or probability of not surviving the disturbance. The complete mission is described through a scenario that is broken down into epochs and actions. The latter can be accomplished through an event tree breakdown (or a kill chain), where the entire incident is broken down into subsequent time epochs. The scenario will help define the survivability equation, and depending on the type of the disturbance, Equation 50 can become:

$$P_S = 1 - (P_H \cdot P_{K/H}) \tag{51}$$

where P_H is the probability of being detected, also known as susceptibility and $P_{K/H}$ is the probability of not surviving the attack hit and get killed after being detected, namely system vulnerability. It is interesting to observe that vulnerability is a conditional probability that depends on the outcome of a threat, while susceptibility is a probability that solely depends on whether the threat was encountered or avoided.

An alternative survivability formulation depends on system *lifetime* distribution, and is widely used in the field of Biostatistics [162]. It is suitable for dynamical systems that undergo longer term effects, and this formulation estimates its survival probability, based on lifecycle calculations. Survivability is expressed through the *survival function*, $S(t)$, which is defined as:

$$S(t) = P(T < t) \tag{52}$$

where t denotes time (assuming $t_0 = 0$), and T is a random variable denoting the time of death. In other words, T, implies the duration of the system being active, or its life expectancy. The survival function is the probability that the system survives for a time period, which is longer than a specified time t. For $t = t_0 = 0$, it is assumed that it is always $S(0) = 1$. Based on the survival function, the *lifetime distribution function* F is the complement of $S(t)$ and is defined:

$$F(t) = P(T \geq t) = 1 - P(T < t) = 1 - S(t) \tag{53}$$

Thus, based on the application of interest and the dynamical characteristics of the system, as well as the uncertainty effects in its operating environment, survivability is formulated accordingly. It can either be a measure of vulnerability to a chain of disruptive events, or the outcome of lifetime distributions, in response to long terms disruptive effects, which determines the system's life expectancy. Proposition 1.1.2 summarizes the role of survivability as a characteristic of resilience.

Proposition 1.1.2: System survivability is a measure of vulnerability, or life expectancy.

4.2.1.2 Attributes of resilient systems

There has been a long lasting debate within the resilience engineering community, regarding a consensus to a commonly accepted definition for resilience, as well as a description of the possible internal mechanisms, that would allow a system to be resilient, according to this definition. For further investigating this matter, Research question RQ1.2 brings emphasis on the resilience attributes, and is expressed as:

Research Question RQ1.2: What are the inherent attributes of resilient systems?

Despite diversity of opinions on term usage when describing the nature resilience, "attributes" is a "working term", that refers to a minimum set of internal, system embedded functionalities, that are responsible for a system to be resilient to threats and uncertainty effects.

As part of the early literature, Holling's definition emphasizes that a resilient system must adopt to change and be able to absorb any adverse effects that result from this change, while maintaining its physical and functional integrity. By this definition formulation, Holling implies that resilient system must perform at least two fundamental functions, the ability to *adapt* to change, and to *absorb*. In a more recent formulation for system resilience by Vugrin et al. [251], there is a third internal function, for the system's ability to *restore* mission operations. Moreover, it is presumed that all dynamical systems, contain a natural capacity to perform each one of these three functions, thus asserting that all systems could be inherently resilient to some extent [111]. As a result, Vugrin et al., refer to the three resilience functions, as *capacities*.

Other literature resources have suggested equivalent resilience function schemes. Retaining the term "function" to describe these resilience capabilities, a resilience functionality scheme has been constructed to summarize SoA findings, and further

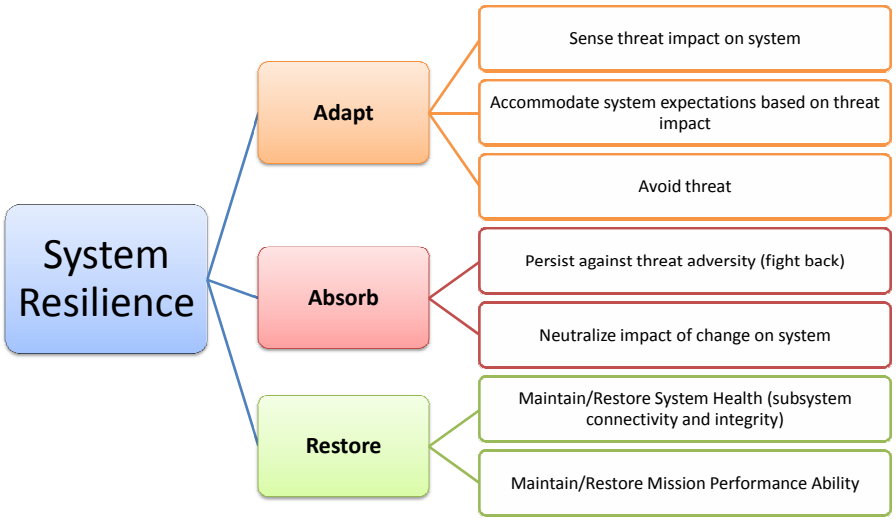


Figure 97: Scheme on resilient system functionality

elaborate on it. The scheme is presented in Figure 97. For the "absorb" function to be activated, it is assumed that the system is experiencing adverse effects due to a threat, which has caused certain dynamic changes on the system. The "absorb" mechanisms either seek ways to neutralize the effects of the threat, or persist against it and fight back.

The "adapt" function on the other hand, is a distinguishing function for system resilience, enabled through a series of lower level functions that support system self-restoration. These range from a sense of self-awareness, and concentrate on either avoiding a threat, or accommodating the system to better adjust to a continuously changing operating environment. "Restore" is a behavioral function, which serves as the basic mechanism for manifesting resilience characteristics. Last, to complement the study of resilience functionality, all three functions have been mapped against similar concepts, in other safety management related disciplines, and the results are presented in Figure 98.

As part of elaborating on the proposed resilience functionality scheme, the three functions will be examined in detail. As observed in Figure 98, the description of

System Resilience Characteristics \ Safety Management Concepts		Robustness	Survivability			Reliability	Security	Basic Resilience
			Susceptibility	Vulnerability	Recoverability			
Adapt	Sense threat impact on system	○	○	◒	○	◒	●	●
	Accommodate system expectations based on threat impact	○	○	◒	○	○	◒	●
	Avoid threat	◒	●	◒	◒	○	●	●
Absorb	Persist against threat adversity (fight back)	●	X	●	◒	○	○	●
	Neutralize impact of change on system	●	X	●	◒	●	●	●
Restore	Maintain/Restore System Health (subsystem connectivity and integrity)	●	X	○	●	●	X	●
	Maintain/Restore Mission Performance Ability	◒	X	X	●	◒	X	○
			Legend	X: N/A		○: Low	◒: Moderate	●: High

Figure 98: Mapping of resilience functionality to safety management concepts

the absorb function relates to system robustness. Even though a concept with great overlap to resilience, system robustness mostly refers to a system's "passive" ability to neutralize or mitigate the adverse effects of a disturbance.

There has been a great debate on drawing the line between robustness and resilience. It has been argued that what the resilience engineering community has been describing as a resilient system, is in fact a robust system architecture. Moreover, experts in system controls and stability argue that most resilience characteristics can be implemented through robust control strategies [98].

However, system robustness and system resilience are not the same. Robust systems are reactive to change, through design-based solutions, such as component redundancy, improved shielding, separated machinery and connectivity. A resilient system would be more proactive for avoiding exposure to the threat, withstanding and recovering from performance degradation. Being proactive requires additional mechanisms for threat discovery and monitoring, system reconfigurability, along with advanced intelligence for decision making. Based on earlier arguments, a resilient system is robust, yet a robust system is not necessarily a resilient system.

To further investigate robustness effects and include them in the resilience assessment, Research Question RQ1.1.1 brings the focus on quantifying the impact of

robustness in dynamical systems:

Research Question RQ1.2.1: How is it possible to quantify robustness effects?

Responding to RQ1.2.1, and in accordance to findings from Figure 98, robustness effects are captured by the "absorb" function, with a capacity that could be estimated, based on performance degradation measures, as Assumption 1.2.1 states below:

Assumption 1.2.1: A dynamical system's ability to absorb the impact of adverse effects, is represented by measure of its performance degradation, for a given level of uncertainty effects.

The system has two options for responding to change under the "absorb" function, either fight back against the adverse effects, or neutralize the impact of change.

Quantifying robustness related effects, is not a very straightforward task. Regarding the recoverability analysis, the metric development was based on a series of observations on dynamical system behavior time histories. To possibly use the same type of source information, to conduct estimates on the system's ability to "absorb" change, a methodological approach is needed. Thus, the Goal-Question-Metric (G-Q-M) method [261] is a systematic procedure for metric development. It has been selected for the development of a quantitative approach for providing estimates on the system's resilience functions. More about the G-Q-M approach can be found in Appendix D.

As a measure of a dynamical system's ability to directly mitigate the effects of change that could lead to performance degradation, the rate at which the system's performance $MC(t)$ is degrading, has been introduced. The average degradation rate ADR is the average time derivative of the loss in performance $\Delta MC(t)$. Thus, ADR is defined for the *degradation time period* Δt_{deg} as:

$$ADR = \Delta MC_{deg}/\Delta t_{deg} \tag{54}$$

with the performance degradation, defined by Equation 41. For the same time period, the *maximum performance degradation* MC_{max} is defined as:

$$MC_{max} = max(MC(t) - MC_0) \tag{55}$$

As a cumulative measure of how well a system can neutralize impact of a threat on itself, the time-averaged performance degradation tMC is defined, and is expressed as:

$$tMC = (1/\tau) \cdot \int_{t_0}^{t_0+\tau} [MC_0 - MC(t)]dt \tag{56}$$

given that $MC(t) \leq MC_0$, for all time instants t, and with τ defined as the total time duration of the captured time histories. An alternative approach suggests a time-weighted, time-averaged estimate $t2MC$:

$$t2MC = (1/\tau^2) \cdot \int_{t_0}^{t_0+\tau} [MC_0 - MC(t)]tdt \tag{57}$$

With this modification, earlier system degradations, penalize more the system's ability to "absorb" the change, as early reactions may be critical for the future evolution of the system state.

In order to establish a better link between the system's "absorb" function, and system robustness, a degradation-to-threat D/T ratio is defined. Earlier metrics only capture the variability of system performance, without any perspective on the intensity of the disruption. This variability is the combined outcome of the performance degradation due to a disruption in normal operating conditions, and the efforts of the system to assist itself and recover its operations. The D/T describes the system's ability to absorb the disruption effect, with respect to the levels of adversity it is encountering.

In order to evaluate the impact of the threat that is causing operation disruptions, and further leading to faults, failures or large scale accidents, the THR levels are defined. The THR however, is specific to the application, and especially on the

types of threats that it describes. To shed more light on threat types and their characteristics, a *threat assessment* is necessary. The goal of this assessment is to characterize the threat, and in most case this involves its deployment in space and time. For instance, a pandemic, a computer virus, a toxic cloud, are all examples of threats, which all have a certain footprint in space, they deploy themselves at certain rates and affect their environment at certain intensities. It is often possible to model the presence and activity of a threat through a threat function d, which is generally expressed as a distribution function $d(x, y, z, t)$. In some cases, spatial variation is independent of its temporal, thus the threat function becomes:

$$d(x, y, z, t) = d_0 \cdot f1(x, y, z) \cdot f2(t) \tag{58}$$

The magnitude d_0 is is the maximum intensity of the threat. The spatial distribution function $f_(1d)(x, y, z)$ is the distribution of the threat intensity in (x,y,z) space, while the amplitude $f_(2d)(t)$ represents the temporal change of threat intensity. Threat severity level THR is a cumulative measure of threat intensity on the system, over a certain time period. To calculate the THR for a system that occupies a certain volume, and is varying in time t, Equation 59 is defined:

$$THR = \int_{t_0}^{t_0+\tau} \int_V [d(x, y, z, t)] dt dV \tag{59}$$

Combining tMC and THR, the signal-to-noise ratio D/T is defined as:

$$(D/T)_{log} = -10 \cdot log_{10}(D/T) = -10 \cdot log_{10}(tMC/THR) \tag{60}$$

A similar path has been followed, in order to extend the framework for evaluating the system's ability to "adapt" to changing conditions. It has been asserted that adaptability is implemented through increased reconfigurability. It is suggested that a system is adaptive, if it can perform at least these three lower level functions:

- Sense threat impact on system

- Avoid threat
- Accommodate system expectations based on threat impact

Except for the sensing function (which falls under situational awareness), the ability of the system to adapt to change and accommodate its mission, its health status to the changing environmental condition, is the most challenging function to implement and to evaluate. The effects of the "adapt" function are incorporated to the total measurable behavior from $MC(t)$ time histories, and cannot be disentangled from the effects of robustness. Going on a lower functional level, threat avoidance is not unique to adaptability, but active system reconfiguration and mission accommodation is a an exclusive adaptivity characteristic. Thus, adaptability evaluation metric development will focus on this particular aspect.

A simple way to investigate the ability of a system to accommodate, is to assess how successfully it can remain within certain performance bounds, or switch to another bounded regime, if deemed necessary. Given a set of prescribed thresholds, adaptability estimates are possible, by calculating time-averaged degradations, with respect to each one of the predefined thresholds.

For instance, if three critical performance thresholds are defined, MC_{negl} (negligible), MC_{marg} (marginal), and MC_{crit} (critical), which describe the severity of the MC degradation, the offsets for $MC(t)$ from these thresholds are defined as follows:

$$\Delta MC_{negl} = MC(t) - MC_{negl} \tag{61}$$

$$\Delta MC_{marg} = MC(t) - MC_{marg} \tag{62}$$

$$\Delta MC_{crit} = MC(t) - MC_{crit} \tag{63}$$

Averaging the offsets over the threat activity duration τ, the cumulative time-averaged threshold offsets are obtained:

$$tMC_{negl} = (1/\tau) \int_{t_0}^{t_0+\tau} [MC_{negl} - MC(t)]dt \tag{64}$$

$$tMC_{marg} = (1/\tau) \int_{t_0}^{t_0+\tau} [MC_{marg} - MC(t)]dt \tag{65}$$

$$tMC_{crit} = (1/\tau) \int_{t_0}^{t_0+\tau} [MC_{crit} - MC(t)]dt \tag{66}$$

The standard threshold values that refer to the offset for the targeted performance value MC_0 from the given thresholds, are defined as:

$$\Delta MC_{negl0} = MC_0 - MC_{negl0} \tag{67}$$

$$\Delta MC_{marg0} = MC_0 - MC_{marg0} \tag{68}$$

$$\Delta MC_{crit0} = MC_0 - MC_{crit0} \tag{69}$$

Then, based on the instantaneous thresholds offsets from Equations 4.2.1.2, 4.2.1.2, and 63, the Relative Threshold Offsets RTO can be obtained, when dividing with the standard offsets:

$$RTO_{negl0} = tMC_{negl0}/\Delta MC_{negl0} \tag{70}$$

$$RTO_{marg0} = tMC_{marg0}/\Delta MC_{marg0} \tag{71}$$

$$RTO_{crit0} = tMC_{crit0}/\Delta MC_{crit0} \tag{72}$$

A cumulative adaptability index can be constructed as a combined weighted average of the three, threshold-based RTO_i offsets. The corresponding Research Question RQ1.2.2 is expressed as:

Research Question RQ1.2.2: How is it possible to quantify adaptability effects? With the support of the adaptability evaluation equations, it is assumed that:

Assumption 1.2.2: A dynamical system's ability to adapt to uncertainty driven changing conditions, is represented by a measure of how well can the system retain its performance degradation above certain critical thresholds.

The third element of resilience, when it comes to its attributes, is system reconfigurability. While reconfigurability is not exclusive to any one of the three resilience functions, it is a characteristic of an architecture that would in theory be capable of supporting all three functions. From Research Question RQ1.2.3:

Research Question RQ1.2.3: How is system reconfigurability enabled?

There are several options for reconfigurability implementation. Some solutions fall under robust design (reactive architectural elements), or some others are software-based (active, intelligence-based solutions). For large scale complex systems, a common approach for system reconfigurability, is through intelligent control strategies. In particular:

Assumption 1.2.3: Reconfigurability is enabled through rule-based intelligent control architectures.

In conclusion for this section, Research Question RQ1 is discussing the theoretical and quantitative formulation, which will serve as the basis of the resilience assessment technique. All necessary elements of resilience have been addressed, from definitions, resilience attributes, functions and characteristics, to quantitative evaluations on a system's ability to be resilient. An overview of the associated responses to research questions and formulated assumptions and hypotheses, is presented in Figure 99.

By combining Premise 1.1, which originates from the investigation of observable resilience characteristics:

Premise 1.1: A resilient system is capable of recovering itself, either by avoiding a

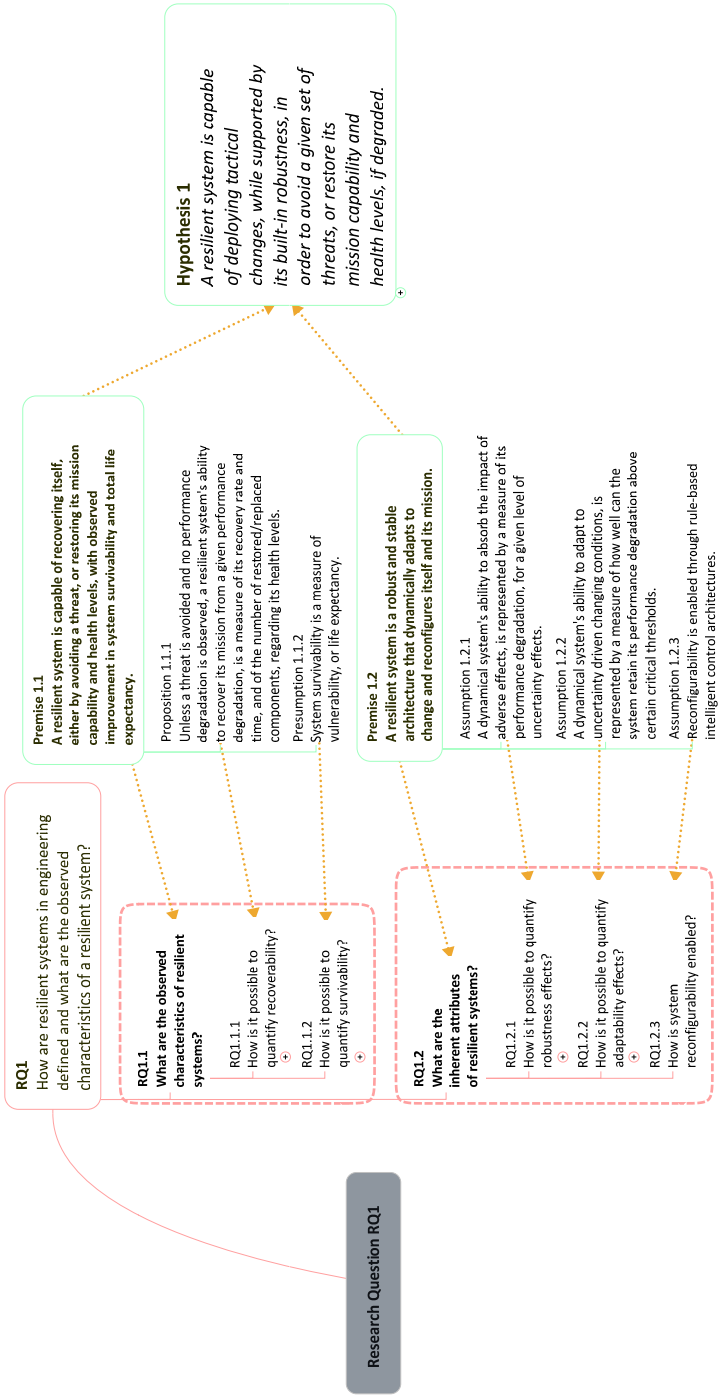


Figure 99: Overview of RQ1 breakdown and proposed research directions

threat, or restoring its mission capability and health levels, with observed improvement in system survivability and total life expectancy. and Premise 1.2, that is addressing resilience attributes:

Premise 1.2: A resilient system is a robust and stable architecture that dynamically adapts to change and reconfigures itself and its mission.

Hypothesis 1 is formulated as an inclusive response to RQ1, which is essentially the proposed definition for a what a resilient system is and does:

Hypothesis 1: A resilient system is capable of deploying tactical changes, while supported by its built-in robustness, in order to avoid a given set of threats, or restore its mission capability and health levels, if degraded.

This is working hypothesis, in support of the upcoming hypotheses, which lead the way for experimentation and testing, as well as for testing the credibility of the proposed resilience definition.

4.2.2 Dynamical system resilience, under the presence of operational uncertainty (RQ2)

Based on the theoretical grounds for this research set by Research Question RQ1, the second RQ2 is concentrated on the resilience assessment problem. This direction is stated by RQ2, as follows:

Research Question RQ2: How are the performance and resilience levels of a dynamical system affected, under the presence of operational uncertainty?

The development of the resilience assessment technique is centered around RQ2, in the sense that it drives the development and testing of the process building blocks. These fundamental blocks are:

1. Operational uncertainty and how is it modeled and included in the process.

2. Dynamical system behavior and performance analysis.

3. Survivability assessment.

4. Variation of resilience attribute capacities.

5. Association of system performance and health status.

4.2.2.1 Operational uncertainty

The presence of uncertainty in dynamical system operations cannot be eliminated. Operational uncertainty triggers disruptions, disturbances, that if combined, can result in larger scale failures or accidents. Uncertainty and its resulting phenomena are integrated to the concept of resilience. From a practical point of view, resilience is manifested through a system's response to the effects of uncertainty. Therefore, a system's dynamic behavior, and its performance must be studied, in order to obtain estimations on resilience capacities. But, before experimenting, certain assumptions are needed, regarding the uncertainty conditions. According to RQ2.1:

Research Question RQ2.1: How are the performance and resilience levels of a dynamical system affected, under the presence of operational uncertainty?

There are several approaches regarding uncertainty modeling, as suggested by the relevant literature. Most modeling methods are used in risk assessment techniques, while the safety and resilience engineering communities concentrate on accident modeling [108]. In military systems, the equivalent approach for addressing uncertainty, is threat assessment and modeling. Last, reliability engineers, typically model uncertainty through faults and failures.

Selecting a technique for uncertainty modeling, depends on the particular engineering application, and the depth at which the assessment study must extend. The outcome of uncertainty analysis provides the input for the assumed conditions, at which dynamic simulations of system operations can be performed. This input is

a collection of certain events, either expected or unexpected (from a system's point of view), occurring serially or concurrently, at different time points and for certain durations (for continuous events). Not only a modeling approach for formulating this collection of events is required, the system simulation model must allow for capturing the effects of these events on system operations.

The resilience concept is advocating for advanced modeling approaches, to better capture expected and unexpected emerging events. Given that resilience engineering itself, is an emerging discipline, and advanced accident modeling is a quite broad area of active research, it is recommended that the resilience concept be first investigated for common types of faults and failures. As progress is made on advanced threat and accident modeling, it would be possible to link the well known forms of faults that reach the system, to the emerging fault causes, which advanced modeling approaches return.

As part of scoping down the focus of this research to a certain part of the uncertainty spectrum, it is assumed that only faults and failures are considered for the experimentation procedures. Thus, Assumption 2.1 states that:

Assumption 2.1: Operational uncertainty is manifested through combinations of faults and performance degradations which could result in system failures or accidents.

The details regarding the types and properties for each assumed fault, depend on the system application and are finalized as part of the experimentation plan. A generalized perspective on threat characterization and modeling, which would result to different types of failures, is available in the Appendix E. Based on this generalized view, Figure 100 contains a set of proposed properties for fault characterization.

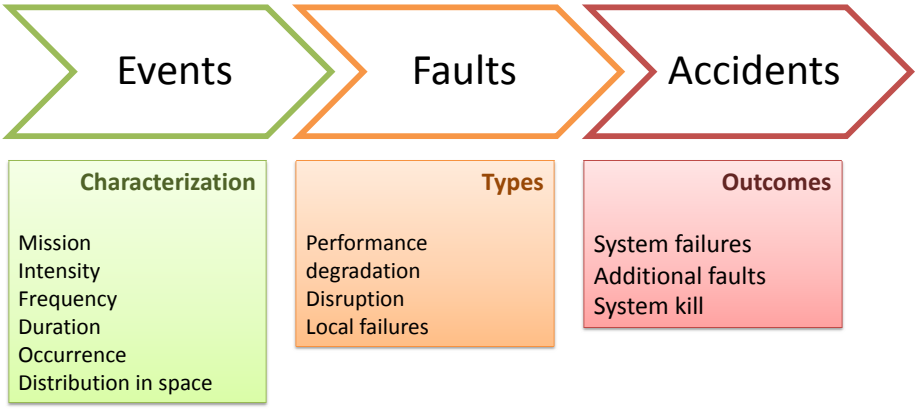


Figure 100: Events for uncertainty modeling

4.2.2.2 Uncertainty impact on performance and survivability

The most critical part of the assessment technique, is the investigation of the uncertainty impact on system performance and its overall dynamic behavior. Research Question 2.2, in particular, brings focus on mission capability, recoverability and survivability:

Research Question RQ2.2: How is operational uncertainty affecting performance, recoverability and survivability?

In order to formulate a response to this research question, it is assumed that the analytical framework of equations under Premises 1.1 and 1.2 is part of the supporting hypothesis. Moreover, Assumption 2.1 regarding uncertainty modeling is taken into account, for the selection of fault types and combinations. Thus, Research Question 2.2.1 is:

Research Question RQ2.2.1: How is performance degradation affected by operational uncertainty, if it depends on fault propagation?

As the literature investigation has revealed, risk assessment techniques are probabilistic. For probabilistic estimations of event outcomes that contribute to overall

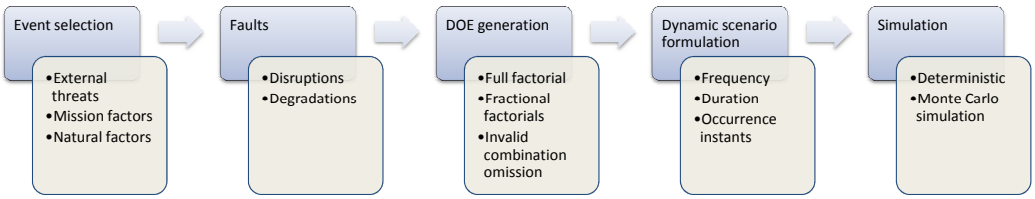


Figure 101: Dynamic scenario formulation procedure

risk, the statistical accuracy depends on the size and the quality of the sample data. It is not only important to formulate several cases for ensuring low statistical error and noise, but one must also properly select these cases, so that the event space is adequately captured.

A commonly used technique to generate cases that describe certain combinations of event, are the *Design Of Experiments* (DOE). The technique allows for experiment planning, through the use of various event combination patterns, in order to better reflect the need of the experiments. Whether the experiment objective is accuracy, screening, data generation for modeling, or a combination of affordability and fidelity, different DoE generation methods are available from the literature.

A *full factorial* design guarantees low statistical errors, but it is usually the most expensive option. For given set of possible events, a full factorial DOE contains experimental cases that represent all possible combinations. However, it is often possible that not all event combinations are valid. Depending on the application and the limitations of the simulation environment, the invalid combinations must be identified and omitted. Screening tests and sensitivity analyses could reveal combinations, that do not significantly contribute to response variability, and thus can be also omitted.

As the dynamic aspect of uncertainty is of high interest, time-based information is necessary for the event combinations. Dynamic scenarios are formulated, by including event frequency, duration, and the time instants at which an event occurs. Last, when probability distributions on event occurrence is available, it is possible to augment the

dynamic scenarios, for accommodating a Monte Carlo simulation. Thus, Hypothesis 2.2.1 is stated as:

Hypothesis H2.2.1: The number of faults, as well as the frequency of fault occurrence, is the primary driver of fault related performance degradation.

An overview of the scenario formulation procedure is presented in Figure 101.

The purpose of planning scenarios for dynamic simulation runs, is to collect data, which will return performance time histories, similar to the one Figure 96. These could refer to the dynamic performance, or health status for each component and subsystem, and for the entire system as well. Analyzing time histories is necessary for the identification of all possible simulation outcomes. Except for total system failure or kill, there could be partial system failures, which correspond to subsystem performance degradations, or total failures. Time history analysis is a key enabler for recoverability estimations, which allow for assessing survivability, with respect to the planned scenario sets, and Research Question RQ2.2.2 is aligned to it:

Research Question RQ2.2.2: How are recoverability and survivability affected by operational uncertainty?

To formulate the hypothesis for RQ2.2.2, a system's notional performance time history for a single disturbance event is considered. Based on the proposed definition (Hypothesis 1), a resilient system is expected to have fully recovered its performance levels, within a required time frame, and eventually surviving through the single disturbance. Based on the idea that a resilient system is robust to a certain extent, the disturbance and its transients must be effectively absorbed. The adaptability mechanism of a resilient system, also ensures that the performance levels will remain above certain mission required thresholds, and that system performance will be restored to its original levels. This notional response is illustrated in Figure 102.

To further elaborate on adaptability effects, another example is brought by Figure

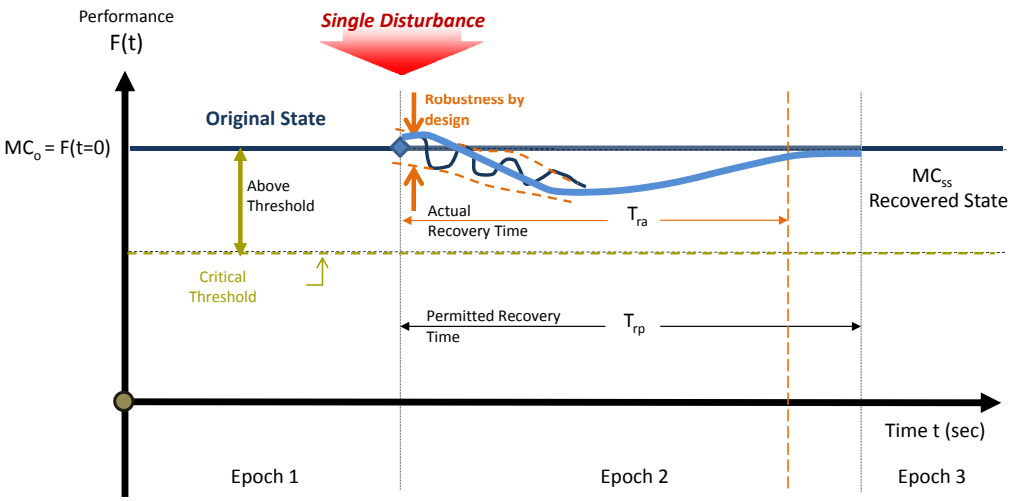


Figure 102: Resilient response to disturbance

103. In the case the disturbance causes a larger degradation, the system's recovery response will follow different paths. The resulting path depends on the location of maximum degradation (minimum performance point), with respect to the critical thresholds, namely the recovery and non-recovery thresholds. For conventional systems with some level of robustness to changing conditions, the maximum degradation point hits the non-recovery threshold, and the system has no chance of restoring its performance (dashed line). Adaptability effects, on a more resilient system, would enable the restoration mechanisms ("restore" function), and the system follows a different path (solid line), towards partial recovery and restoration of its original performance.

If, however, the system is not robust to disturbances and cannot adapt to earlier thresholds, it will reach the (ultimate) failure threshold. The absence of resilience functions and mechanisms could result in a total catastrophic system failure, even if some recovery was achieved for a short period, as it is shown in Figure 104.

Summarizing the ideas that have been discussed, the response to RQ2.2.2, is Hypothesis 2.2.2:

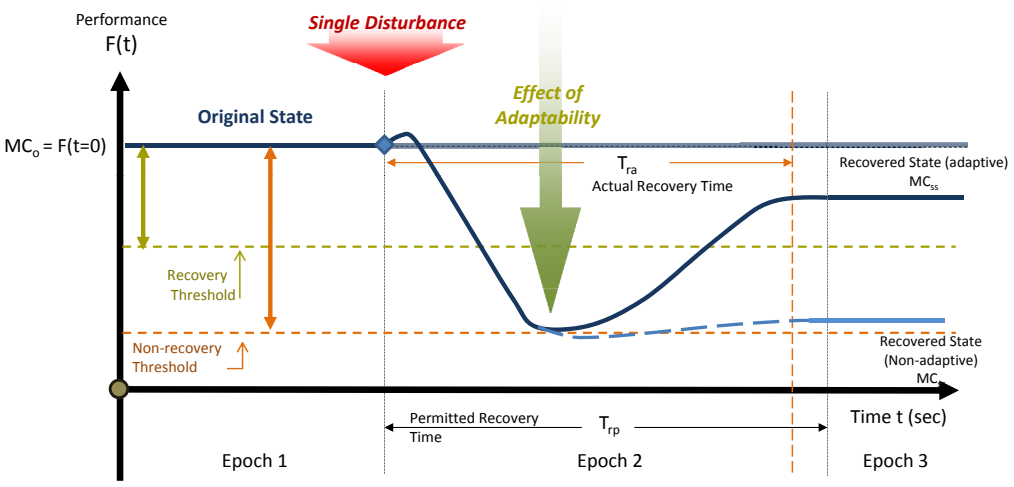


Figure 103: Effects of adaptability on partially recovery from single disturbance

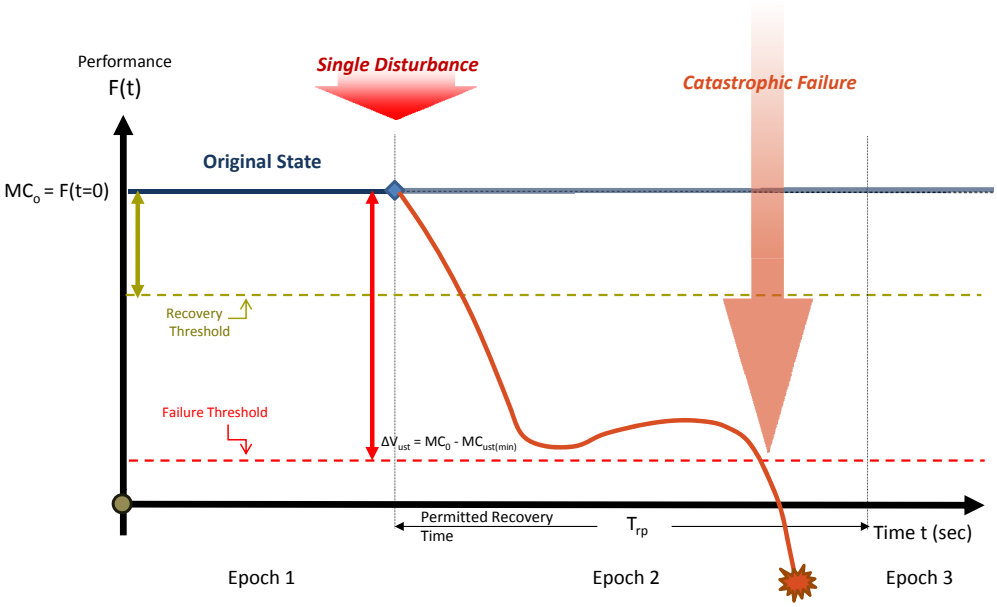


Figure 104: Catastrophic failure response to disturbance

Hypothesis H2.2.2: For dynamical systems with certain robust solutions (by-design, e.g. redundancy, intelligent control), survivability is less affected by the number and frequency of faults.

Last, the closing hypothesis 2.2, in response to RQ2.2, is based on combining Hypotheses 2.2.1 and 2.2.2, along with prior intuition on dynamical system responses to external disturbances:

Hypothesis H2.2: Being representative of the operational uncertainty, fault density and frequency mostly drive the system's performance degradation, yet with less impact on survivability, for robust and resilient designs.

4.2.2.3 Uncertainty impact on resilience attributes

Within the context of the theoretical formulation, in support of Hypothesis 1, a functional breakdown for a resilient system response has been proposed. Given that three basic functions are what a resilient system is expected to perform, a set of equations has been developed, in order to describe the system's capability to perform these functions. The essence of the metrics reflects the capacity of a system to perform the three functions. In particular

- The "restore" function capacity is described by the average recovery rate, and the comparison of the restoration value to the original levels of performance.
- The "absorb" function capacity is described by time-weighted average estimations of performance recovery and through a signal-to-noise ratio, in comparison to the external input threat or disturbance levels.
- The "adapt" function capacity is described by time-weighted estimations of how well system performance can remain above a threshold or within certain performance boundaries.

With the capacities linked to the proposed metrics for resilience assessment, the next point of interest is to investigate the impact of uncertainty on the resilience capacities. As Research Question RQ2.3 states:

Research Question RQ2.3:How are the resilience capacities varying, in the presence of operational uncertainty?

RQ2.3 is broken down to address capacities for adaptability ("adapt") and robustness ("absorb"), under RQ2.3.1:

Research Question RQ2.3.1: What is the correlation between dynamical system resilience and operational uncertainty?

as well as recoverability ("restore") and survivability, through RQ2.3.2:

Research Question RQ2.3.2: How are resilience capacities affecting system survivability and recoverability?

There is not adequate evidence from the literature, for formulating a hypothesis on RQ2.3. The identification of variation trends for the resilience capacities against operational uncertainty, is an open question for the resilience engineering community [251]. The formulation of Hypothesis 2.3 will be based on the general response expectations for resilient systems. If one goes by the proposed definition of Hypothesis 3.1, resilient systems are expected to be flexible to changing operating conditions. As such systems must absorb the effects of change on their performance, it would make great sense to assume that it must also vary its capacities of performing the "adapt, "absorb", and "restore" functions, as part of this flexibility and response readiness. Thus Hypothesis 2.3.1 is formulated as:

Hypothesis H2.3.1: As part of their inherent flexibility, resilience systems adapt to changing conditions, and absorb the impact of uncertainty, thus resilience capacities depend on operational uncertainty.

With support evidence on Hypothesis 2.3.1, RQ2.3.2 captures the essence of RQ2.3, and one of the fundamental goals of this dissertation. This goal is to demonstrate that resilient systems (in accordance to the presumed definition) are more survivable to conditions created by a large range of disturbance scenarios, given that they are capable deploying the "adapt-absorb-restore" functionality. Thus Hypothesis H2.3.2 summarizes this point:

Hypothesis H2.3.2: The presence of resilience, either through the ability to adapt to change, or avoid/absorb the impact of change, improves system survivability and recoverability.

In response to H2.3.1 and H2.3.1, Hypothesis 2.3 states that the system resilience capacities, contribute to improving recoverability and survivability, yet they are affected by operational uncertainty:

Hypothesis H2.3: For resilient systems, resilience capacities are affected by operational uncertainty, and they contribute towards improving survivability and recoverability.

Summarizing Hypotheses 2.1, 2.2, and 2.3, Hypothesis 2 is formulated as response to Research Question 2, regarding the effects of uncertainty on resilience capacities and system survivability.

Hypothesis 2: Under the presence of operational uncertainty,in the form of faults and performance degradations, system resilience ensures and augments the necessary levels of survivability and recoverability, with a self-adjusted, synergistic relationship between system capability and health levels.

The proposed plan and scheduled research work for Research Question RQ2, is summarized in Figure 105.

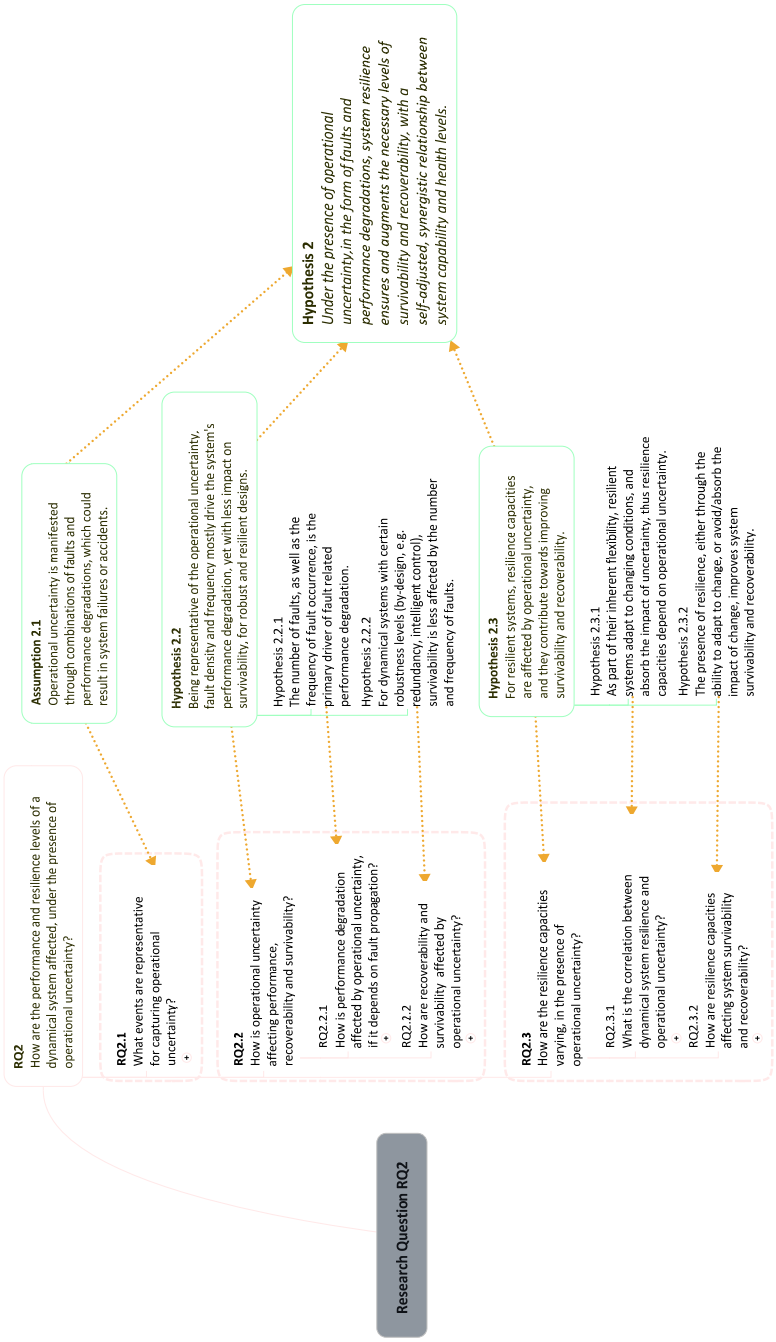


Figure 105: Overview of RQ2 and the associated proposed plan

4.2.3 Architecture enhancement for more resilient systems (RQ3)

In accordance to the framework that has been presented thus far, the levels of system resilience are evaluated according to the system's ability to perform three basic functions, at the occurrence of single, or multiple disturbances. This ability is quantitatively expressed through the capacities of performing the "adapt-absorb-restore" functions. Absorptive and adaptive capacities are critical for initial stages of disruptions, where system repairs may be impossible in the short term, thus prioritizing restorative capacity to build up in the long term after the disruptive event. While adaptability and robustness allow for a system to be insensitive to a disturbance or neutralize its effects, they cannot always guarantee recovery. Thus restorative capacity of a system depends upon its interdependency to other systems and the inner reconfiguration strategies. However, there is a big question regarding the dependence of such capacities and thus system resilience to a particular sequence of events.

Vugrin et al. argue that capacities for performing the three resilience functions may be highly correlated for different disturbance events. Event timing and time constants of the system response to disruptions also play an important role on capacities and resilience. According to Hypothesis 2.3, and Hypothesis 1, a resilient system is expected to be independent of the event uncertainty. There still may be correlation which is affected by uncertainty, but resilience capacities must remain independent. As consequence, there is a need for design and optimization approaches, which would seek to ensure that these capacities are at a necessary level for resilient system responses, and that they are maintained against operational uncertainty. Design methods would introduce solutions and technology enhancements on the system architecture for this purpose. It is necessary to investigate how such enhancements would contribute to overall resilience under uncertainty. This research objective is expressed through the third research question RQ3:

Research Question RQ3: How do architecture enhancements affect the resilience and effectiveness levels for dynamical systems, under the presence of operational uncertainty?

4.2.3.1 Options for improving system resilience

As resilience is a concept that is differently interpreted by different entities, similar observations hold regarding the suggested strategies towards improving system resilience [193]. For instance, aircraft safety and survivability engineers, advise for redundant critical subsystems [18]. Naval architects also advocate for system redundancy, spatial separation and physical partitioning within a ship architecture [26]. Researchers on vehicle dynamics and controls recommend special robust controllers that ensure adaptability and stability, also known as resilient controllers [98]. Last, network and communication engineers would design and optimize for alternate information transmission paths, to avoid breaches and lack of communication between critical subsystems [248]. Thus, possible resilience enhancements depend on the type of the system, internal subsystem connections and physical topology.

Except for design-based solutions, there can be technology infusion for improving resilience. Taking a biology-inspired approach, a technology acts as an "antibiotic" in system health management. Embedded system technologies serve to both actively monitor and enhance a system's resilience, by extending absorptive and adaptive capacities. A separate set of technologies and functions could focus on restorative capacity, in a fashion similar to how a human body restores basic functions after an infection has been isolated and neutralized. To implement such functionality, automation and intelligent control must be combined with reconfigurable architectures [207]. Thus, Research Question RQ3.1 is addressing this need:

Research Question RQ3.1: What enhancements must be considered for improving adaptability and robustness to change due to operational uncertainty?

For enhancing overall system resilience, the literature has returned a set of options, of which a list with most common possible recommendations is presented in the following:

- Redundant critical components (e.g., auxiliary power generators, strategically selected service loads for large scale power systems).
- Strategic placement of components within the topology.
- Automation and intelligence, through adaptive, rule-based control architectures.
- Reconfigurability architecting solutions for strategic and mission specific power and resource allocation.

Taking into account all these options, experimentation will concentrate on component redundancy, and rule-based control architectures, as well as reconfigurability, as it is partially linked to either one of the two approaches. As a result, it is asserted that the tested approaches will include the following:

Assertion 3.1: With adaptability and robustness as key enablers for system resilience, possible enhancement solutions resort to intelligent control architecture design, as well as advanced topologies, with subsystem redundancy, strategic spatial allocation for mission reconfigurability.

4.2.3.2 Effects of enhancements

Hypothesis 3.1 has introduced the enablers for enhancing system resilience, as part of the experimentation process. Given that the main idea behind RQ3 is to investigate and quantify the impact of these enhancements to system resilience capacities and survivability. This goal is addressed by Research Question RQ3.2:

Research Question RQ3.2: What is the impact of resilience enhancements on system survivability and recoverability?

RQ2.3 is broken down to RQ2.3.1 and RQ2.3.2, in order to address the enhancement strategies to be considered, namely topology modifications and implementation of rule-based control architecture, respectively.

Research Question RQ3.2.1: How do architecture modifications for improved robustness affect system resilience?

Robust design encompasses decision making for configuration selection, which ensures that system performance levels are less affected by the noise, that is induced by variability in changing operating conditions. Based on this particular view of robustness, the goal for R.Q3.2.1 is to evaluate alternative configurations, through the proposed resilience assessment approach. Resilience evaluation and assessment is the preliminary step, in order to support a resilience-based design method for resilient configuration selection.

The alternative route to design for robustness, is to develop intelligent control architectures. This direction is stated through Research Question RQ3.2.2:

Research Question RQ3.2.2: How does a rule based control architecture improve system resilience?

The literature offers great wealth of knowledge on this field, in the form of robust control design, large scale control architectures, artificial intelligence, and others. The idea behind intelligent control, is to improve system reconfigurability, with less investment on extending the size and the physical complexity of the architecture, while improving the logic behind the automated actions and overall flexibility of the system. With this approach, equivalent performance and robustness to noise could be achieved, with less hardware-based investment, but with improved logic and intelligence.

In order to illustrate the expected impact of enhancements, either in the form of topology modifications, or intelligent, rule-based control architectures, a notional

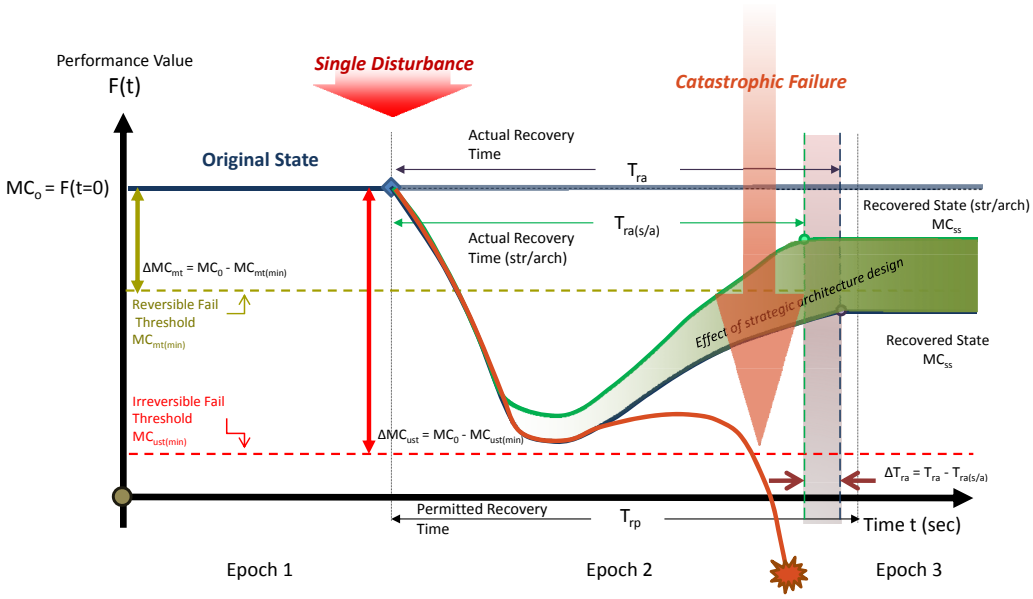


Figure 106: Comparison of notional responses to a single disturbance, with and without resilient architecting

example is presented, based on the system response of Figures 103, and 104. As Figure 104 suggests, the occurrence of a single disturbance, may have such impact on the system, where it progressively degrades, and fails to remain above the failure threshold, resulting in a catastrophic failure. If the system was robust to disturbances of this type and intensity, or carry additional capabilities for reconfiguring itself, and effectively reacting to the disturbance, it could potentially hold itself above other higher safety thresholds. In most cases, this could guarantee its dynamic stability and it would allow itself to avoid the catastrophic failure and restore its performance (and health) to a value close to the original. This is the basic goal of either one of the enhancing enablers, and a notional schematic for this targeted, stable dynamic behavior for system recovery, is shown in Figure 106.

Based on the earlier notional example on resilient system response, Hypotheses 3.2.1 and 3.2.1 have been formulated, in order to test the recoverable dynamic response of systems, that are robust by-design, or employ rule-based control strategies:

Hypothesis 3.2.1: Enabling robust design solutions on system topology, improves

system resilience, through recoverability, as a consequence of better ability to absorb the effects of a disturbance.

Hypothesis 3.2.2 concentrates on enabling control strategies for recovery, without a robust design to be necessary:

Hypothesis 3.2.2: Enabling intelligent or rule-based control solutions on system architectures, improves system resilience, through recoverability, as a consequence of better ability to adapt to changing conditions, that are induced by the effects of a disturbance.

Therefore, after taking Hypotheses H3.2.1 and H3.2.2 into account, the final Hypothesis 3.2 to be tested is a formulated as:

Hypothesis H3.2: More resilient architectures demonstrate extended life expectancies, improved system survivability and recoverability.

4.2.3.3 Cost considerations

The support of Hypothesis 3.2, along with its supporting Hypotheses 3.2.1. and 3.2.2, raises the significant issue of the tradeoff between investment on resilience enhancements, against the actual effectiveness of these solutions, to resilience, and survivability. The investment includes costs of installation (e.g. redundant subsystems), retrofitting (if architecture modifications are required) for accommodating systems and technologies, as well as development costs, either for technologies, or control-based solutions. In any case, costs are incurred if architecture enhancements are planned, not only for installation, but also for maintenance and running operations. Last, costs appear in the form of system performance downgrades, or incompatibility with certain system operations, at the expense of improving resilience. To illustrate this point, redundant components or power transmission lines allow a power grid to

be more resilient against unexpected incidents, such as extreme weather, natural disasters, etc. At the expense of a more resilient network, the applies enhancements add to acquisition and maintenance costs, while accounting for additional weight and space occupancy, that may eventually negatively affect power output and efficiency.

Current robust design techniques ensure that the system maintain its expected performance, under the presence of environmental and operational variability. The range of the variability is often assumed and determined in the design process. Robustness however, must be ensured in the case of unexpected variability, which may be beyond the assumed boundaries the system has been configured for. To address unexpected, but possible uncertainty, is sometimes a common practice to "overdesign" a system, especially for systems that are of crucial mission importance.

With the term "overdesign", one could refer to extensive redundancy throughout the architecture, excessive use of strong, durable and sometimes expensive materials, or increased overall complexity. This practice is found in military vehicle design (e.g. a HMMVEE), where the additional armor, ammunition and weaponry result to increased acquisition and maintenance costs, along with the associated operational complexity. Performance may be degraded, if excessive weight is a critical factor, while the system may lose some of its expected agility and maneuverability, and furthermore result to susceptibility increase. On the positive side, this practice can actually support vulnerability reduction, not necessarily by-design, but through extensive use of technology and active solutions onboard. It is practice that is based on the idea, that addition of equipment, or technology solutions is proportional to vulnerability reduction, thus improving survivability.

The "overdesign" practice may often be effective, fast and easy to implement, but it does not always result to efficient design configurations. As part of the accepted compromise, the yield in performance and flexibility may pose a number of unexpected risks. For instance, robust design are optimized for maintaining their operations

under unexpected (but predicted) conditions, but they are not always capable of self-restoring system health and mission operations, when unexpected and unpredicted operating conditions are present. As resilient systems are expected to demonstrate capabilities on anticipating both predicted and unpredicted conditions, future resilient system design and optimization methods must address options for avoiding system "overdesign". Cost consideration is the basis for investigating design, performance and resilience compromise, and is addressed through Research Question RQ3.3:

Research Question RQ3.3: What are the cost implications for more resilient designs?

In order to set the ground for exploring this research objective, certain propositions are introduced. Based on certain evidence that designing for resilience is a compromise among different system responses, correlation of these responses must be explored. System health and mission capability are two responses of interest. If for certain systems, health degradation does affect mission performance, then one could assume that health and mission capability are dependent, and their association can be represented through 2-D scatter or trajectory plots. Assuming that dynamic responses for mission capability and system health follow the degradation and recovery behavior of that in 102, the combined dynamic response, allows for the "trajectory" to be formed, as explained in Figure 107.

A particular trajectory represents a given system design configuration. The relationship between mission capability and health in the presence of operational uncertainty, is a trajectory that follows different paths, as a consequence of varying operating conditions. As a given system configuration exhibits a certain behavior, the corresponding trajectory of a given configuration follows a unique path, which is depends on its mission requirements, operational uncertainty and the design characteristics of the configuration. If design characteristics relate to the resilience functions

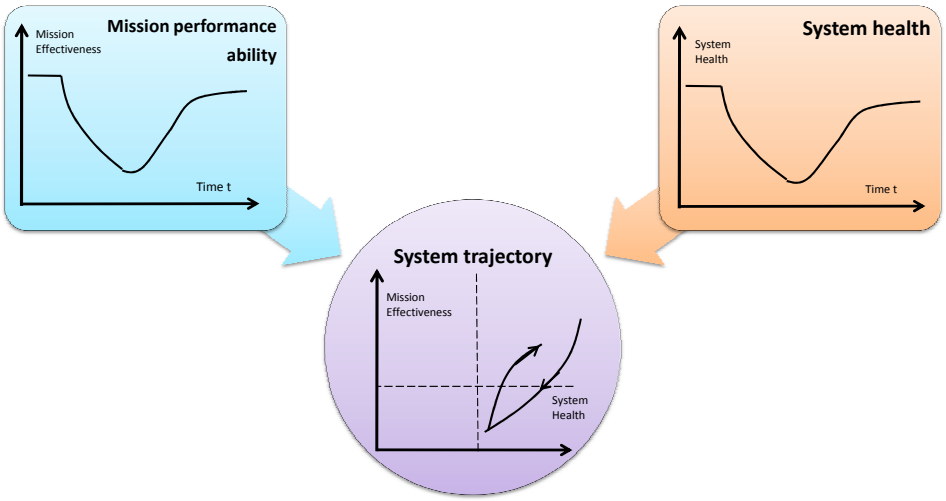


Figure 107: Formulation of system mission-health trajectories

and their capacities, the 2-D trajectories are representative of the system's resilient response, in the presence of uncertainty. For 2-D mission-health graphs, with single constraints for each response, there are four possible outcomes, as the notional graph of Figure 108 suggests.

For systems that are characterized of certain resilience capacities for the "adapt-absorb-restore" functionality, trajectory plots could reveal additional information, regarding recoverability for the mission and the system's health, the restoration points, as well as the shape of the recovery path. Figure 109 displays three different types of trajectories, under combinations mission requirements and operational uncertainty, for a fixed system design. In terms of better survivability, the closed trajectory is the preferred one, given that system health and mission capability both degrade, but are both recovered to their original states, with the possible support of resilience mechanisms. Regardless of whether the requirement imposed constraints are violated, another trajectory type, is the partially recoverable system, which does not restore its health and mission capability to the original values. Last, it is possible to degrade at values below the constraints, where the system possibly fails to recover and restore its health and mission.

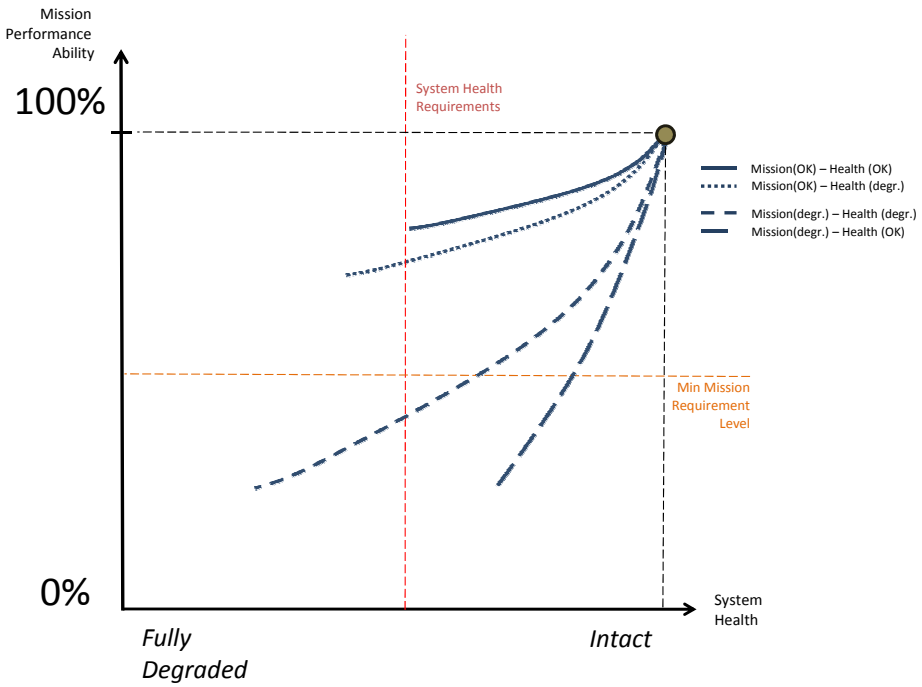


Figure 108: Trajectory plots for system-mission performance

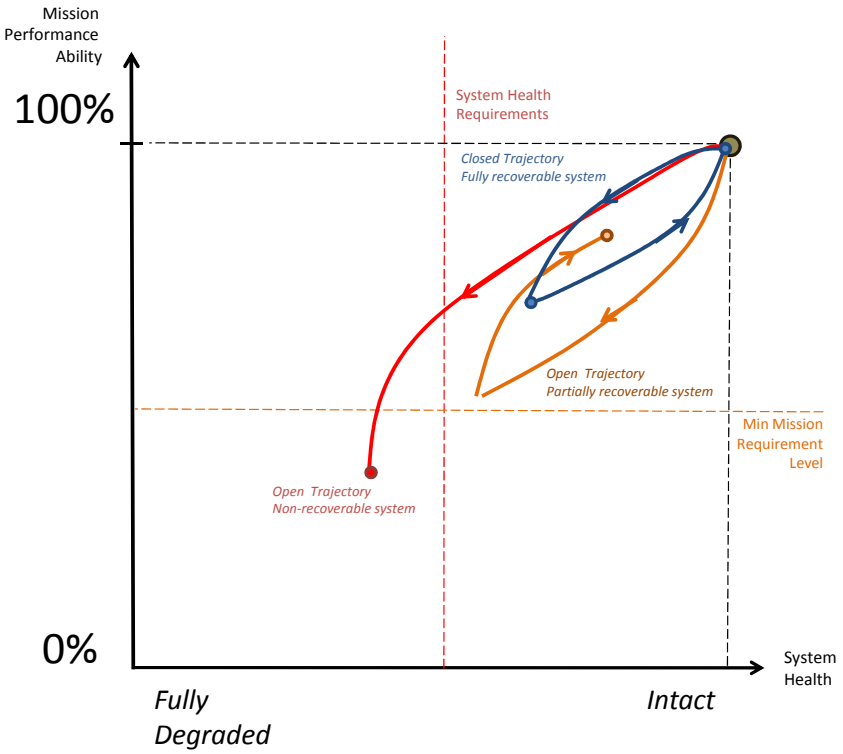


Figure 109: Recovery paths for resilient systems

It would be interesting to investigate and assert the trajectory shapes, which would correspond to the different aspects of a resilient system. Robustness effects, would manifest themselves through shorter degradation paths, with possible partial or full recovery, in accordance to the robustness characteristic, of the ability to "absorb" uncertainty-induced noise effects. A resilient response would be additionally characterized of improved recoverability and adaptability, thus it would be the one that allows for full system recovery, at a minimum. Except for its contribution to recovery and ability to absorb uncertainty effects, adaptability would manifest itself, as the internal mechanism that allows for full recovery and restoration, even if the system momentarily violates either one of the mission or health constraints. Last, if one brings the ideas behind costs and efficiency, a resilient system must fully recover itself with minimum degradations, by choosing the shortest recovery path, in a fashion similar to reversible processes. Concentrating all previous thoughts, Hypothesis 3.3 can be formed:

Hypothesis H3.3: In contrast to robust design, which may return expensive, over-capable design configurations that ensure minimum degradation, resilience-based design is exploring affordable configurations, which possess right-sized capacities for the "adapt-absorb-restore" functionality, with the objectives of minimum capability and health degradation due to uncertainty, full recovery and restoration, as well as short recovery paths.

To summarize this section on RQ3, hypothesis H3 can be expressed as:

Hypothesis H3: Enhancements, such as subsystem redundancy, strategic spatial allocation and mission reconfigurability contribute to more resilient architectures, that demonstrate smaller degradations in mission capability and system health, yet all benefits come at some cost in weight and expenses, or implementation time.

Concluding, the proposed plan and scheduled research work for Research Question

RQ3, is summarized in Figure 110.

4.3 Overview of the experimentation plan

With the research directions and deliverables having been set in the previous sections, it necessary to formulate an experimentation plan. According to the scientific method, a series of experiments must be planned for supporting the research hypotheses [151]. Elaboration on the research questions, did not necessarily result to testable hypotheses only, as certain premises, assumptions and propositions have been necessary for building the top-level hypotheses, which address the main three research questions. An overview of the research hypotheses, along with supporting presumptions, propositions and assertions for this dissertation is presented in Figure 111.

The experimentation plan brings all necessary elements together, for hypothesis support, the development and the demonstration of the resilience assessment methodology. These include the simulation models for experimentation, the experiment and a first approach on the resilience assessment process.

4.3.1 Canonical problem for assessment technique development

The motivation for this research has been inspired by the problem of naval survivability. With resilience engineering to become one of the enabling frameworks for improving system survivability, it would make great sense to test and demonstrate resilience engineering methods on complex naval system problems. For method development and hypothesis support, however, the high degree of complexity of a large scale naval system architecture is not the most suitable. To improve experimentation and the understanding of the observed outcomes, a smaller scale, but equivalent dynamical system problem is recommended.

For this purpose, a small scale dynamic problem has been formulated and implemented, in order to be used as a pilot problem for proof-of-concept and method development. The canonical problem is a multi-element spring-mass-damper system

Figure 110: Overview of RQ3 and the associated proposed plan

Figure 111: Summary of research hypotheses

Characteristic		Canonical Problem	Large scale dynamic system
Mission description	Operation	Support load distributions	Perform a series of functions
	Protection	Withstand external forces and impulses	Withstand external disruptions, attacks and other threats
Environmental factors	Space	Distributed/concentrated loading	External: Missile or torpedo Internal: Fire, disruption, malfunction
	Time	Periodic/non-periodic loading	Recurrent/One time threat
Physical system behavior	Threat suppression	Elasticity, damping, control of structure	Advanced technologies safety equipment, robust design
	Damage generation and propagation	Material strength limits, natural degradation, fatigue,	Component damage, multiple points of initial damage, loss of operability
	Recoverability	Smart material, redistributable loading, flexible control	Reconfigurability, redundancy, modularity, flexible control architecture
	Adaptability	Adaptive control	Resilient system design

Figure 112: Equivalence between canonical and large scale naval systems

configuration, which oscillates under the input of external time-dependent forces (with pulse or periodic signals). The configuration however for the canonical problem has not been randomly selected. Based on intuition from operating and experimenting with naval system model simulation environments, there is a minimum set of characteristics, that describe dynamical systems. This mostly refers to the dynamics and reconfigurability of power systems and cooling networks of a ship architecture. It is required that the canonical problem capture dynamic transients in their state variables, as well as the level of reconfigurability of a larger network. It must also model damage and possible cascading effects for damage propagation. The impact of environmental factors must be also modeled, with time-dependent and space distributed external inputs. As naval systems are tasked to perform certain missions, a canonical problem must carry similar tasks, and have the external inputs act as disturbances towards their mission. A summary of the modeled characteristics for the canonical problem is provided in Figure 112.

Returning to the canonical problem model, it is a single degree-of-freedom spring-mass-damper (SMD) system, which experiences external force disturbances of varying

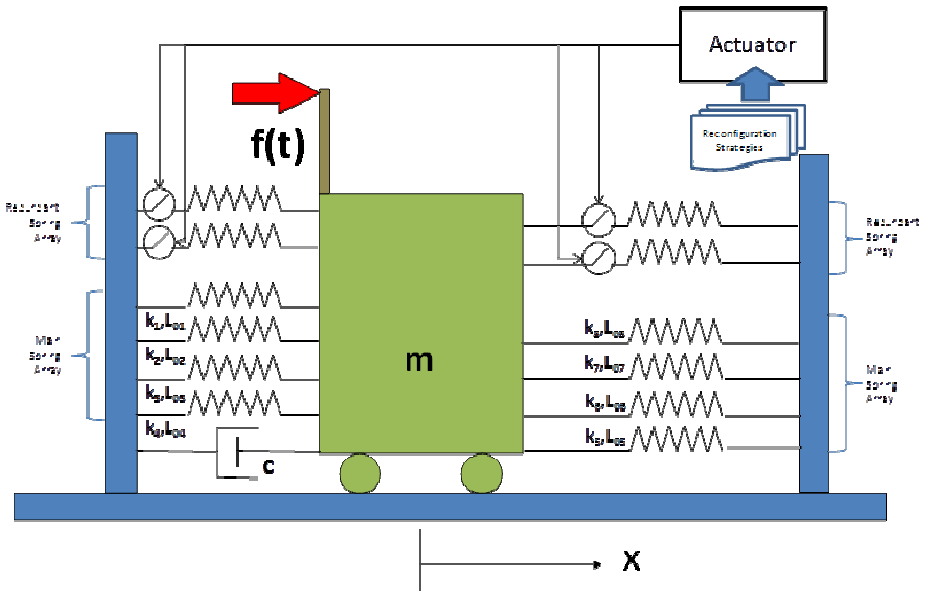


Figure 113: Canonical problem for investigating system resilience

amplitude, frequency and duration. The system configuration is shown in Figure 113. Energy is stored and exchanged through an array of eight main springs. The basic "mission" for this system, is to ensure that the mass m remains within certain boundaries, as it oscillates on horizontal x axis. The combination of the spring array and the damper mechanism, is configured for ensuring that the system does not move out of bounds.

As part of the system's "mission", there is a nominal force of fixed magnitude, which drives the oscillation. For capturing the effects of operational uncertainty, there is an additional external force which disturbs the system and tends to push the mass out of bounds. Both the damper and the spring array, are expected to concurrently generate the opposing forces, which will compensate for the external "threat" force. The damper is responsible for dissipating the energy added on the system, due to the disturbance, while the springs generate the opposing forces to the disturbance. These mechanisms result in the system's dynamical behavior in the form of its oscillation $x(t)$. The system's mission capability levels are dependent on this

oscillatory behavior.

To allow for resilience investigation, the model must allow for component health monitoring. To keep the model simple, the elements that exhibit vulnerability, are the main springs of this setting. The springs are characterized by certain levels of stiffness, which must not exceed the given thresholds, if "healthy" operation has to be maintained. This form of vulnerability, is a consequence of the material strength of the springs. Depending on spring material or physical characteristics, the health thresholds are determined by the limit and the ultimate loads that the springs can withstand without breaking.

In the case that either one of these thresholds are exceeded, the corresponding springs experience degraded stiffness, and a subsequent total breakage occurs. To avoid this possibility, the system is equipped with a rule-based classic feedback controller, which is responsible for monitoring normal spring operation, as well as their "health" status. System reconfigurability is allowed through an additional array of four springs, that can be activated by the control system. If certain springs degrade and partially operate, or are broken, the controller takes action by activating one or more springs from the redundant spring array. Total system stiffness is increased, with the goal of restoring the initial total spring stiffness, and effectively restoring the system's "health".

4.3.2 Reconfigurable cooling network architecture for technique demonstration

The purpose of the SMD canonical problem model is to be the pilot application for the resilience assessment technique development. A different application however, has been selected for demonstrating the resilience assessment technique. This task is necessary for indicating the relevance of the proposed approach, to the original problem and motivation, that both refer to naval system applications. For maintaining simplicity and better transparency, but without losing in generality, a small

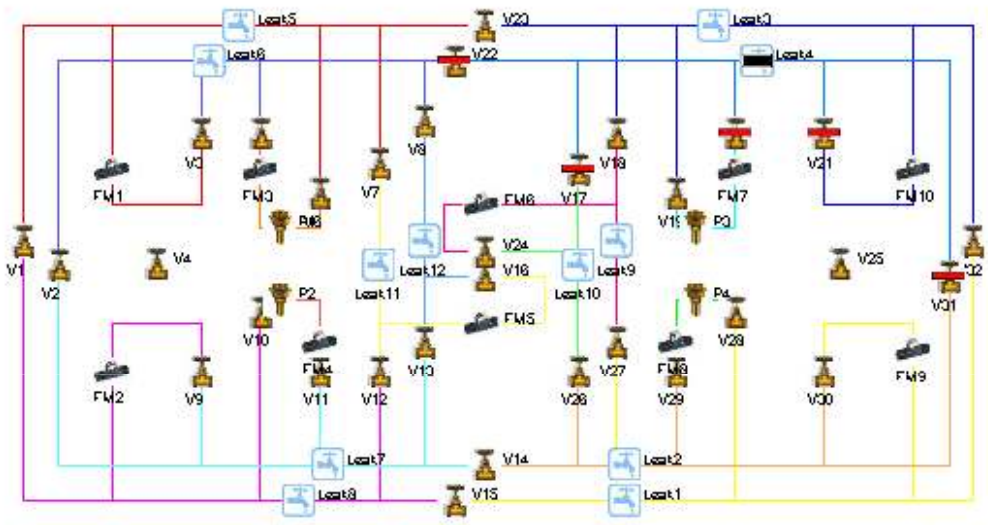


Figure 114: Chilled water network for resilience assessment technique demonstration

scale naval system application is selected. The chilled-water demonstrator model has been developed by Icosystem Corporation [179] and JHU APL, allows for dynamic simulation of cooling network operations, with a view of the network shown in Figure 114. The particular configuration is a smaller scale version of a similar chilled water system of a full size naval combatant.

The necessary dynamic characteristic requirements for this type of system are outlined in Figure 112, essentially being the basic characteristics of complex hierarchical, dynamical systems, that operate in hostile, disruptive and uncertain environmental conditions. As it is shown in Figure 114, besides the fundamental elements of a cooling network, such as combinations of pipes, valves, and water pumps, the architecture has the ability to monitor critical performance outputs, such flow rates and control flow in different parts of the network, through a number of control valves. The valves are controlled by a simple, rule-based, ideal response controller, which has been developed by Icosystem Corporation, and has been provided with the current model implementation [179].

As the requirements in dynamical behavior are captured by this model, the particular implementation is capable of modeling leaks on the network. Network leaks represent the effects of uncertainty through the changing environmental conditions. Leaks can occur at specific time instants, as well as in different physical locations on the network. However, this leak model is not commanding for recurring events, but for fixed time and location, and fixed rate, non-removable leaks. Multiple leaks can be considered, thus all combinations for the possible leak locations are allowed. As a response to leak events, the controller decides which valves must be closed, so that the network regions that contain a leak are isolated from the rest of the network.

4.3.3 Experiments

The planned experiments for the investigation of Hypotheses 2 and 3 are divided into two groups. The first group, is addressing Hypotheses 2.2, 2.3.1 and 2.3.2 and involves experiments that investigate the effects of uncertainty on observed responses, such as performance, recoverability and survivability, as well as the impact on the resilience capacities for the "adapt-absorb-restore" functionality. The second group is focusing on Hypothesis 3, as well as the specific Hypotheses 3.2.1, 3.2.2, and 3.3, with experiments on investigating the impact of resilience enhancements on both observed responses and resilience capacities, as well as tradeoffs between response variable combinations.

In the following, the full set of experiments is conducted with the canonical problem, in support of the resilience assessment technique development. The same experiment sets will then be conducted with the naval small-scale problem, as part of demonstrating the technique, and supporting its relevancy to the naval survivability problem. Chapter 5 presents the results and findings from canonical problem experiments, whereas Chapter 6 contains the demonstration with the small scale naval system problem.

4.3.3.1 Experiments for RQ2

As explained in earlier sections, operational uncertainty is manifested through events, that have certain impact on normal system operation. An event could trigger adverse effects on system performance, recoverability, and further impact system survivability, and resilience. The goal for RQ2 is to investigate these uncertainty effects, thus the appropriate experiments must be planned.

Operational uncertainty is varying according to the event characteristics, such as frequency of occurrence, amplitude, direction, duration, and others that capture special aspects of the uncertainty induced events. Earlier observations from experiments have indicated that the variability of these input characteristics, results in varying responses regarding dynamical system performance and stability.

With these facts in mind, Hypothesis 2.2 implies that varying input settings for uncertainty factors must result in response variability in performance and resilience measures. Experiment 1.1 is formulated to test this Hypothesis:

Experiment 1.1: Perform Monte Carlo Simulations with the system baseline (fixed architecture, fixed control and reconfiguration strategy), under varying uncertainty factor settings. With the response data, generate a series of scatter plot diagrams and investigate the relationship between uncertainty factors and recoverability and survivability responses. Recoverability is described through recovery rate, recovery time, restoration value offset, and survivability depends on life expectancy time durations, which returns survivability estimates through survival times.

Hypothesis 2.2 is false under the following two conditions:

1. System recovery and survivability are insensitive to the assumed uncertainty factor variability

2. Frequency and duration are not the most significant uncertainty factors, to

system recovery and survivability.

For the canonical problem, the uncertainty factors include the magnitude, frequency, duration and occurrence of the disturbance input force. Variability in the mission required input force is also assumed. For the demonstration problem, uncertainty factors include the number of leaks, and their locations.

Hypothesis 2.3 brings focus on a research topic, without any prior knowledge available. The validity of Hypothesis 2.3 is less accurate, but Experiments 1.2 and 1.3 will shed more light on it. The goal is to investigate the effects of uncertainty on the presumed resilience capacities for the "adapt-absorb-restore" functions. This is stated through Hypothesis 2.3.1 and Experiment 1.2:

Experiment 1.2: Using the experiment data from Experiment 1.1, perform calculations for the resilience capacities. Generate and analyze the relationship between the varying uncertainty input factors and the resilience capacities.

Hypothesis 2.3.1 is false under the following condition:

1. Uncertainty effects keep the resilience capacities unaffected.

To complement Hypothesis 2.3.1, Hypothesis 2.3.2 indicates that the variability of resilience capacities under uncertainty, is necessary for maintaining better recovery and survivability.

Experiment 1.3: Using the experiment data from Experiments 1.1 and 1.2, investigate the tradeoffs between resilience capacities and the levels of recovery and survivability.

Hypothesis 2.3.2 is false under the following two conditions:

1. Recovery and survivability do not vary with resilience capacities.

2. Recovery and survivability do not improve with resilience capacities.

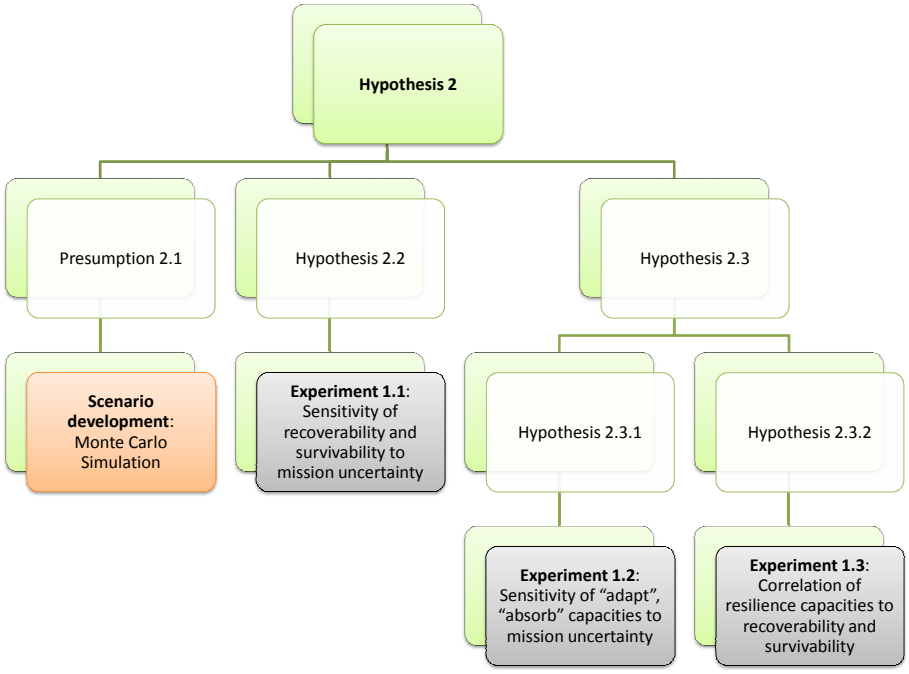


Figure 115: Experiments for Hypothesis 2 support

Concluding the experimentation plan for RQ2, Experiments 1.1, 1.2 and 1.3 are presented in Figure 115.

4.3.3.2 Experiments for RQ3

The research objective with RQ3, is to investigate the effects of architecture modifications and enhancements, on system recovery, survivability, and the resilience capacities. Modifications for resilience enhancement are organized into two groups:

1. Physical architecture modifications (e.g. redundancy, separation, or damage suppression solutions)

2. Control architecture modifications (e.g. control scheme, reaction rules and strategies)

In order to statistically ensure the reliability of the results, uncertainty effects for this investigation are the same as the ones assumed for Experiments 1.1, 1.2 and 1.3.

Hypothesis 3.2 is the central hypothesis for addressing RQ3. Hypothesis 3.2.1, involves investigation of the impact of architecture modifications on recoverability and survivability. Further exploration includes resilience capacities. Thus Experiment 1.4 is expressed as:

Experiment 1.4: Incorporate robustness enhancing solutions through physical architecture modifications. Execute the Monte Carlo simulations with the same uncertainty settings, as in Experiment 1.1 Based on response data, estimate recovery and survivability and track the tradeoffs with the direction of modification improvement. Analyze the resilience capacities and investigate their correlation with the modifications.

Hypothesis 3.2.1 is false under the following two conditions:

1. Robustness improving modifications do not improve survivability and recoverability

2. Robustness improving modifications do not improve any one of the three resilience capacities.

For the canonical problem, physical architecture modifications for robustness, are effectively represented through different damping values. For the demonstration problem, robustness improvement is performed through the generation of network architectures with varying total number of control valves.

As a complement to Hypothesis 3.2.1, Hypothesis 3.2.2 similarly supports the idea that intelligent control architectures, or sophisticated rule-based control strategies can improve survivability and resilience. Experiment 1.5 is quite similar to Experiment 1.4, with the only difference that there are no physical system modifications, but experimentation with different control strategies:

Experiment 1.5: Generate a set of different control strategies and run an equal number of Monte Carlo simulation, with the same uncertainty input settings as in Experiments 1.1, 1.2, 1.3, and 1.4. Based on response data, estimate recovery and survivability, while identifying which strategies improve these estimates. Analyze the resilience capacities and investigate their correlation with the different control strategies.

Hypothesis 3.2.2 is false under the following two conditions:

1. Control strategy modifications do not improve survivability and recoverability
2. Control strategy modifications do not improve any one of the three resilience capacities.

For the canonical problem, control strategy modifications are represented by the response algorithm, that decides on how redundant springs are being activated, as a result of broken or inactive main springs. For the demonstration problem, the effects of control architecture are investigated through two simulation runs, one with and the other without the presence of the control system.

With RQ3.3 directing to a potential integration of the resilience assessment technique, as a key part of a resilience-based design and optimization methodology, the final Experiment 1.6, brings the aspect of cost. As argued earlier, cost implications can be discovered by investigating the relationship between mission capability and system health. This is performed through the mission-system trajectories, and it is asserted that system resilience effects are implicitly present through these trajectories. Thus Experiment 1.6 is described as:

Experiment 1.6: Using the response data from the enhancement studies of Experiments 1.4 and 1.5., combine mission capability and system health calculations to formulate the mission-health trajectories. Demonstrate the variation of these curves,

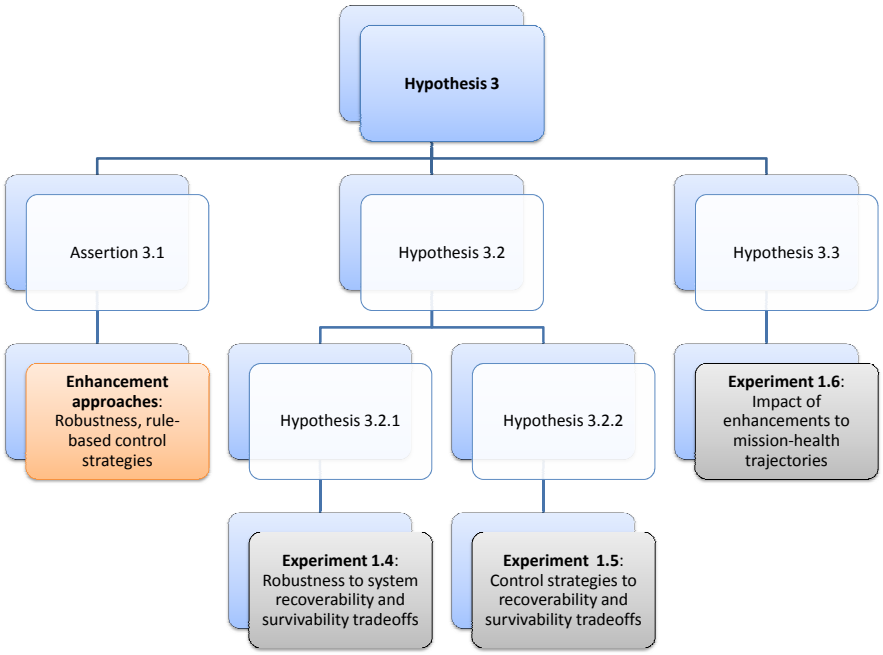


Figure 116: Experiments for Hypothesis 3 support

for the given modifications. Identify the combination that returns the assumed "better" resilient response, based on the trajectory curve assertions. Finally, compare the selection to the corresponding resilience capacity estimations.

Hypothesis 3.3 is false under the following condition:

1. Shortest trajectories do not correspond to better resilience capacities

A summary of the planned experiments under Hypothesis 3, is presented in Figure 116.

CHAPTER V

DEVELOPMENT OF A PROBABILISTIC RESILIENCE ASSESSMENT TECHNIQUE

The experimentation plan that has been proposed in the previous chapter is the bassi for the development of the resilience assessment technique. For this purpose, a small scale pilot problem has been formulated, while results and findings from small scale experiments will become the building blocks for the assessment process. The technique will then be further developed in fine-tuned with a larger scale naval problem.

5.1 Introduction to the proposed Probabilistic Resilience Assessment Technique

With the finalization of the experimentation plan, along with the research hypotheses that it supports, this Chapter is presenting the initial findings, from putting the plan into practice, The core of the plan is the development and testing of a probabilistic resilience assessment technique. The technique has been christened after Tiresias [93], a famous Greek oracle that is known from ancient Greek mythology and had a unique ability, despite his blindness to foresee future events and warn on post-event developments, thus allowing the people that trusted his vision to be proactive and to better prepare themselves for what is bound to happen. To a great extent, the scope of this methodology is to provide similar information on what can happen to a given baseline architecture, if it experiences certain events and changes on its configuration. As the technique's acronym, TIRESIAS stands for: "Topological Investigation for Resilient and Effective Systems through Increased Architecture Survivability." An overview of the proposed methodology is illustrated in Figure 117.

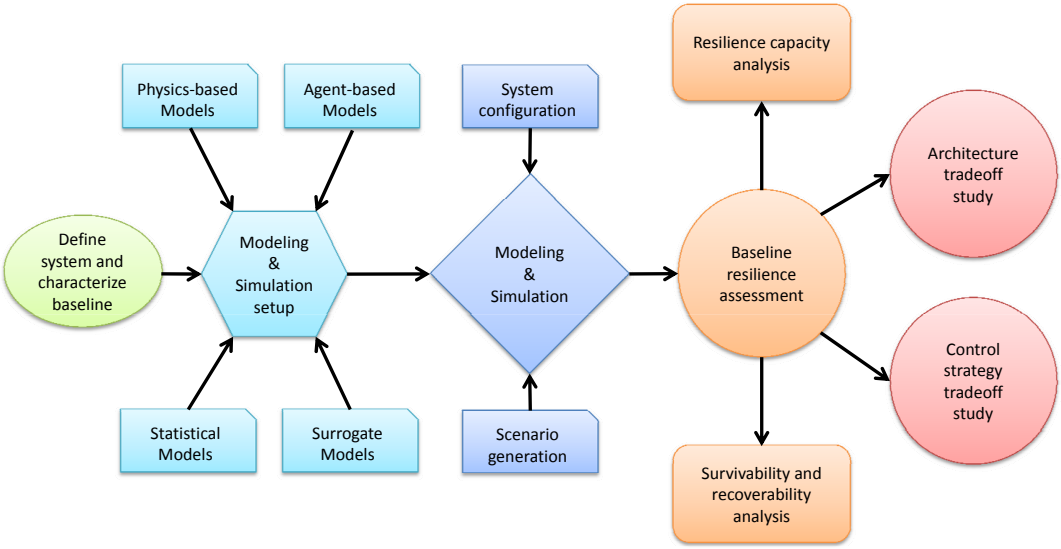


Figure 117: TIRESIAS for system resilience assessment

5.1.1 Step 1 - Define and characterize system baseline

The starting point of the method is to define the system, its functions and its topology. For multidisciplinary systems, it is necessary to identify all relevant engineering domains (e.g. electrical, mechanical, structural, etc.), while the stakeholder requirements provide for mission objectives, desired capabilities and limitations, that usually reflect physical and financial constraints. Physical and functional system characterization must return the system state variables and performance response metrics, which are relevant to the particular engineering application and to the stakeholder requirements. Depending on the particular problem, system variable mappings to system resilience variables are necessary.

5.1.2 Step 2 - Set up the Modeling & Simulation

A Modeling & Simulation environment must be set up for experimentation. Depending on the requirements of the study, and the available resources, there are several

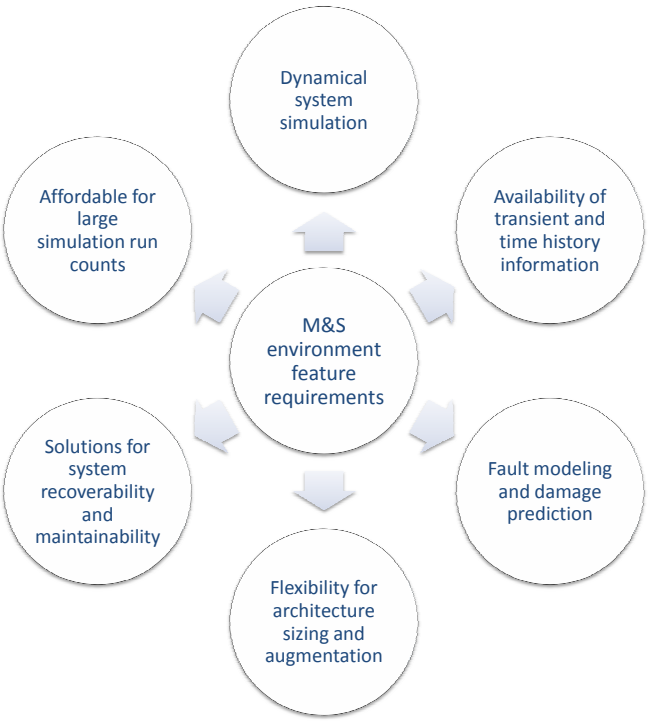


Figure 118: Features of Modeling & Simulation environment

options, from which the building blocks of a computational simulation tool can be obtained. Most commonly chosen options are physics-based computational models, agent-based models, statistical models, and surrogate models, if at least one of the earlier options is available. Despite the possible options, the selection of a suitable facility is not always straightforward, especially when affordability constraints become effective. The latter factor is quite significant for probabilistic analysis methods, given that they typically depend on large numbers of simulation runs, especially for Monte Carlo type simulations.

Figure 118 describes the minimum capabilities for the simulation environment. Based on the selected canonical problem, as well the case study for the technique demonstration, the previous figure underlines the equivalent features for both problem formulations, in accordance to the simulation expectations. The expected simulation responses include time histories for subsystems and component performance,

which are relevant to the system's overall mission performance ability and system health. Depending on the application, other simulation capabilities include models for changing environmental conditions, as well as damage estimation and propagation prediction models.

5.1.3 Step 3 - Create mission/threat profiles and formulate scenarios

In dynamical system analysis, where dynamic stability, survivability, reliability and availability are of major concern, it is necessary to define an external stimulus, which either in the form of imposed disturbance, fault, failure, or other form of disruption is affecting normal system operations. The stimulus could be the manifestation of naturally changing environmental conditions, or the presence of a threat. Changing environmental conditions represent uncertainty in system operations, and rely on mostly random variability of environmental parameters. A threat however, is a more sophisticated form of stimulus, and prior analysis of threat possibilities may be necessary.

Appendix E contains some basic proposed guidelines for threat analysis. Threat analysis results can be summarized in a threat morphological matrix. This matrix contains threat profile information, as well as possible combinations of threats, while it is helpful in decision making for threat combination selection [130]. Uncertainty and threat attributes that will be considered for this study are summarized in Figure 119.

Following the threat analysis and possible options, the last deliverable of this step is the preparation of experimental scenario cases. The cases are produced as arrays, which contain the corresponding input settings. Depending on the planned study, the input settings could reflect different sources of variability. The input settings, according to the particular prospective study can belong to one, or more of the following groups:

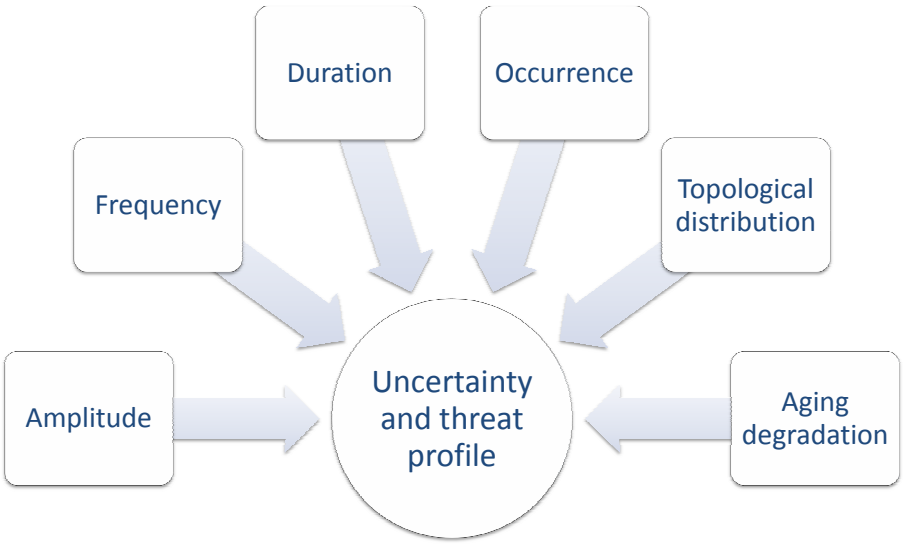


Figure 119: Uncertainty and threat attributes

- Settings for variability due to environmental uncertainty.
- Settings for faults, and operations variability due to threat effects and failures.
- Settings for architecture variability due to sizing and design modifications.
- Settings for control strategy variability through reconfigurability.

Using *Design of Experiments* (DoEs), is a great choice for generating the combinations of input settings, which will then constitute the series of simulation scenarios for the experiments. When cost of runs is not a major issue, a full factorial design is the most complete option, for capturing most of the combinatorial space. Other DoE options of reduced size are also applicable, in the case that the number of simulation runs is limited. Another source of possible scenario size reduction, is the identification and removal of incompatible or problem irrelevant combinations for the input factors, according to event compatibility on the particular application study. Ideally, a DoE with the minimum number of scenarios and meaningful event combinations, that can capture most of the response variability, is the most favorable choice for scenario formulation. For the planned experiments, a Monte Carlo simulation approach has

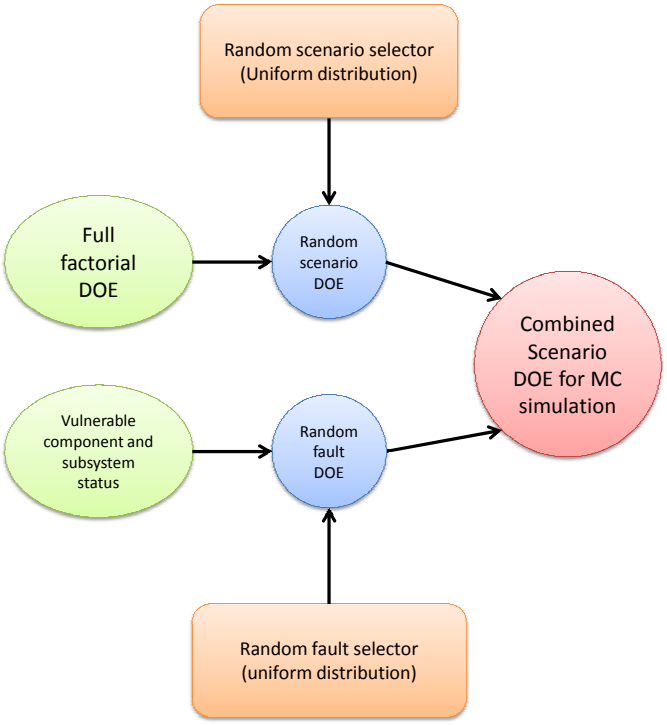


Figure 120: Scenario formulation approach

been selected. The process for the scenario formulation regarding the Monte Carlo experiments on the canonical problem, is a combination of a fractional factorial, along with random scenario selector, as explained through Figure 120.

5.1.4 Step 4 - Resilience & Survivability Assessment for system baseline

With the availability of a working M&S environment, along with the necessary scenario input sets, the first exercise is to perform the resilience assessment on the baseline design. The return of quantitative results on how the system performs against mission uncertainty and external variability will serve as a reference point, in further studies where possible directions of improvement are investigated.

Baseline resilience and survivability analysis depends on system performance time histories, which is the outcome of the executed experiments. In particular, the following responses are required:

- Real-time capability measurements (e.g. power delivery on power systems, flow

rates on cooling networks, displacement, velocity, or acceleration for mechanical systems).

- Real-time system health measurements (e.g. subsystem or component operating status, or capability measures that also apply for health monitoring).
- Life time measurements (e.g. duration of system operations, event or epoch durations).
- Real-time damage propagation information (e.g. damage location data, or propagation rates based on damage prediction models, or capability and health measurement analysis). enditemize It is not necessary that these essential measurements are independent of each other. Depending on the system under study, it is often possible to derive certain measurement types from prime capability or health measurement with a proper analysis procedure.

As all the required real-time information is collected and properly processed and stored, the following four tasks are performed within the baseline resilience analysis:

1. Survivability analysis.
2. Life distribution analysis.
3. Damage propagation analysis.
4. Resilience capacity analysis.

Given that task execution depends on the availability of the supporting data, it is not always possible to perform all the analyses. The resilience capacity analysis, however, is the core of the resilience assessment technique, thus data availability for this particular task must be always ensured.

Survivability and lie distribution analysis, requires event and epoch duration data, and returns survivability probabilistic estimates that could be compared to the resilience capacities. Last, damage propagation analysis is often integrated with a damage prediction model, that is part of the M&S facility. If time duration data cannot be extracted from performance or health monitoring information, then damage analysis is another potential source. Depending on the system that is being considered, damage propagation analysis could return measurements and estimations for health monitoring.

Resilience capacity analysis involves all background measurements, for supporting estimates on the system's ability to perform the three proposed resilience functions, namely adapt, absorb, and restore. Observed and analysis derived estimates on recoverability, robustness to noise and adverse effects, as well as system state transition through critical threshold, are representative of the system's capacities to restore itself, absorb effects of change, and adapt to change respectively. The number of experimental cases that were executed for uncertainty analysis, must be sufficient for reliable statistical estimates on the three function capacities, and allow for correlation and design space exploration studies.

5.1.5 Step 5 - Tradeoffs with system architecture and control strategy modifications

The last step of the method, builds upon the assessment procedure for the baseline, and expands into investigating the effects of architecture modifications on system resilience. This step is necessary for the exploration of possible architecture enhancements that benefit overall system resilience and survivability, and constitutes the link between the assessment technique, and a prospective resilience-based design space exploration and optimization methodology.

In theory, there should not be any limitations on the classes of possible enhancements that could be tested. The key enabler however, is one again the capability of

the M&S environment. In other words, the simulation facility must allow for modeling of the effects of a tested solution, at the level of performance and time duration responses, at least. For instance, survivability enhancement exercises through architecture modifications, command for simulation models of modular and customizable system architectures. As long as the M&S facility allows for it, the same resilience analysis procedure can be executed, with the study results to be compared to the baseline responses. For the current research plan, two classes of architecture modifications are considered:

1. Architecture modifications for robustness, through redundancy and flexibility.

2. Control strategy modifications for leveraging system reconfigurability.

In the following sections, the results of the application of the 5-step procedure are presented, as they have been performed for the canonical system. The exercise serves as a process for research hypothesis investigation and support, and as a preliminary demonstration of the technique, before its application on a large scale system is introduced.

5.2 Experimental setup for the canonical system study

The canonical problem is a spring-mass-damper (SMD) system, in a parallel connected, multiple-spring configuration. It is a small scale model, as part of an engineering study problem, that is used as a "pilot" application for methods testing and development for the resilience assessment technique. The design for the system baseline configurations has been selected with the following criteria in mind:

- Dynamical system with dynamic responses and behavior that is fairly comparable and analogous to the behavior of larger scale and more complex dynamical systems.

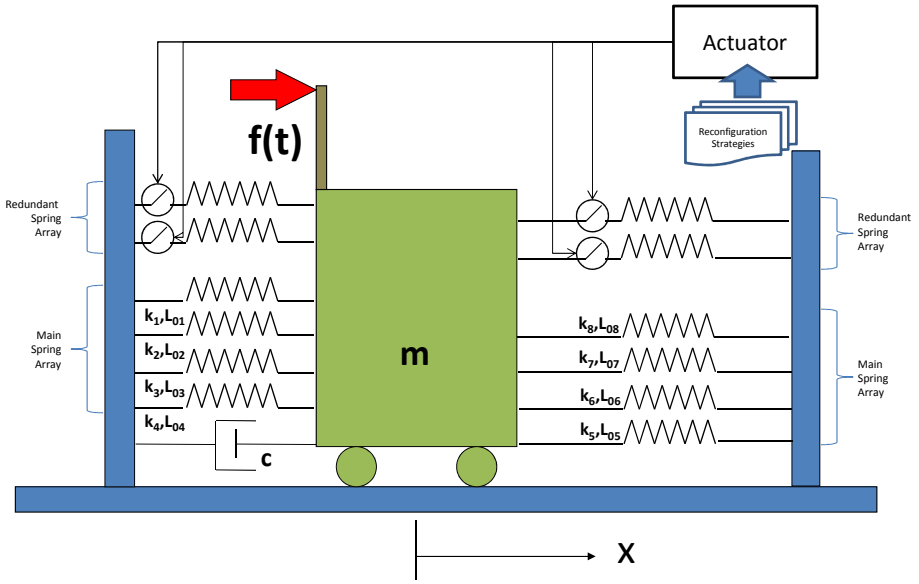


Figure 121: Canonical problem for investigating system resilience

- The description, modeling approach and behavior responses must all be well understood and explained.
- The selected configuration must be scalable, modular and easily reconfigurable.
- Modeling approach and implementation must be kept simple and transparent.
- Simulation runs must not be expensive to execute (time and setup efforts).
- The configuration must allow for incorporating additional modules, such as controllers, or other input types.

The SMD system is a single degree-of-freedom (SDOF) model, which allows for its mass to oscillate in a range, that is bounded on both sides. The selected configuration is shown in Figure 121 consists of the moving mass, a damper and eight springs of different lengths L_{0i} and spring constants k_i. Moreover, there is an array of four additional, redundant springs, which can become connected to the mass, when the control system commands for it. A notional actuator is also part of the system, and is responsible for executing the commands that it receives from the feedback

controller in real time. Last, the fixed parameter settings for the SMD system model are presented in Table 2.

Table 2: Input parameter values

Parameter	Variable	Value
Mass (kgr)	m	10
Damping ratio	CTRL	0.02
Spring length (m)	L0	0.03
Spring diameter (m)	D	0.01
Young's Modulus (N/m2)	E	207e9
Yield strength (cast iron) (Nm-2)	sigma_y	200e6

In a more abstract sense, the "mission" of the system, is to avoid excessively large oscillations and remain within its boundaries of operation. This mission could be performed without interruption, if there weren't additional, "unexpected" input forces, which add energy on the system, and could potentially drive the mass to the boundaries, while inducing extreme stresses on the springs. The spring modeling approach includes a performance degradation module, that downgrades spring stiffness, when certain input force thresholds are met or exceeded.

There are two types of forces that act as external stimuli for perturbing the system. First, there is a nominal constant force of amplitude p_0, that can be adjusted according to the system's mission. The second external input force of amplitude d_0 plays the role of an "unexpected" disturbance, thus essentially capturing the effects of environmental uncertainty in system operations. The shape of the disturbance dynamic input signal is adjustable, to either be a step function or a sine wave. The core of the SMD modeling approach is a single DOF, second order ODE, that is numerically solved in MATLAB/Simulink, and is the basis of the analysis of system vibration. More information and details regarding the analytical modeling approach is found in Appendix F.

The association of resilient systems to adaptability and robustness to changing conditions has been underlined and is a critical ingredient of the research hypothesis

formulation. In order to capture the effects of an adaptive and reconfigurable system, a feedback controller, is programmed to ensure that the proper level of total stiffness is available to the system at all times. The selected values for spring stiffness, for both main and redundant springs are presented in Table 3.

Table 3: Spring stiffness values for main and redundant springs

Spring Constant	Stiffness (kN/m)	Crit. degr. force (kN)	Rate lambda (sec-1)
Main k01	2	2.5	2
Main k02	2.5	3	2.5
Main k03	2.5	2	2.5
Main k04	2	3.5	2
Redn k01	2.5	2.8	2.5
Redn k02	2.5	2	2.5
Main k05	2	1	2
Main k06	2.5	2	2.5
Main k07	2.5	2	2.5
Main k08	2	3	2
Redn k01	2.5	2.8	2.5
Redn k02	2.5	2.5	2.5

In order to set up the experimentation cases, the variables that represent the effects of uncertainty through their variation, must be selected. Taking into account the particular characteristics of the SMD model, the primary variables that control the vibration of the mass, are the frequency f of the disturbance input signal (if the sine wave shape is selected), as well as the signal's amplitude d_0. With respect to event timing, additional uncertainty factors are the disturbance force occurrence time point t_{init}, as well as the duration τ of the signal. Last, operational uncertainty is also represented by the level of expected variation within a mission, thus another layer of variability is added with the nominal mission input force p_0. The settings for the uncertainty factor variables are shown in Table 4.

In the case of larger scale systems, with available topology information, one can include the location of disturbance activity, as well as its distribution in space, for the case of continuous, non-concentrated threats. Each setting combination represents a

Table 4: Input variable range settings for DOE generation

	Mission input	Disturbance input	Occurrence time	Duration	Frequency
	p_0 (kN)	d_0 (kN)	t_init (sec)	tau (sec)	f (Hz)
Min	1	1	0.1	0.5	1
Max	10	1000	0.2	1.5	100

unique "threat" level (and is represented by a THR value). It must be noted however, that the uncertainty factor breakdown is dependent upon the particular dynamic and physical characteristics of the system, thus the variable and input value selection for uncertainty factors is not an automated process, and must be performed by the designer.

Formulation of the scenario cases has been based on combining a full factorial DOE with a random case selector. The full factorial DOE generation returned a total count of 385 unique scenario cases. Then, a random number generator (adhering to a uniform distribution) selects a certain scenario case, thus creating a total of 2000 cases, in support of executing a Monte Carlo simulation. Each case is executed for a simulation time of $t_{sim} = 5$ sec.

Every single simulation case returns a fixed set of output responses. Starting from the physics of the system, time histories for displacement, velocity, and acceleration data is available. The three responses are the basis for deriving additional information, that will be linked to mission capability and system health. A typical time dependent response, that describes the system's vibration is shown in Figure 122 for the baseline case.

As explained earlier, mission capability in dynamical systems, is a measure of the system's ability to adjust its actual performance level, to a mission commanded target performance level. For the SMD system, the mission capability $MC(t)$ is a function of the envelope of oscillation $xmax(t)$, defined by Equation 73.

$$x_{max}(t) = max(x(t)) \tag{73}$$

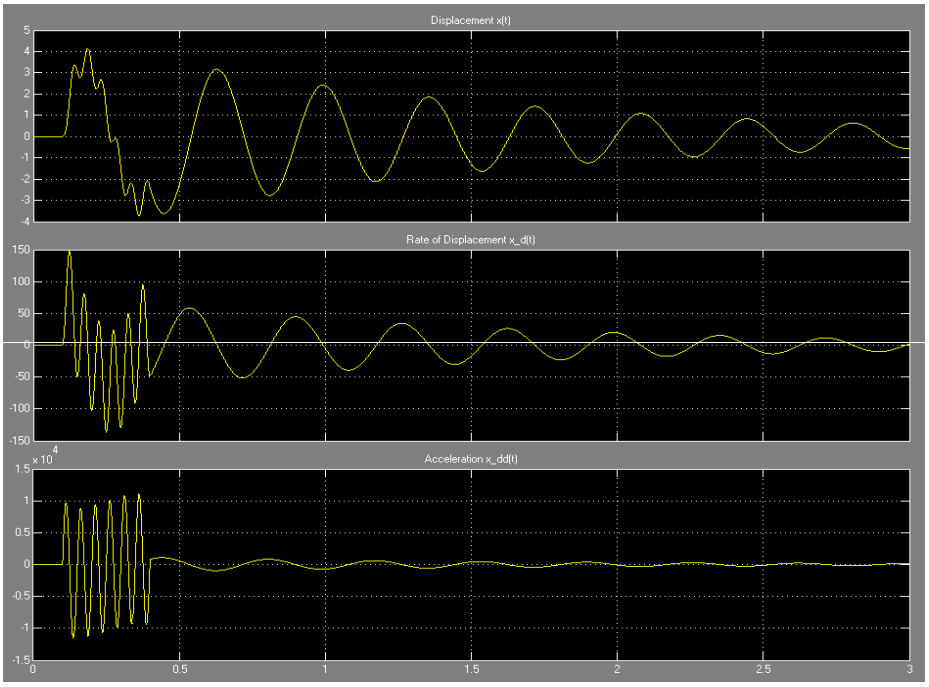


Figure 122: Time histories (in sec) of system responses (displacement, rate of displacement and acceleration)

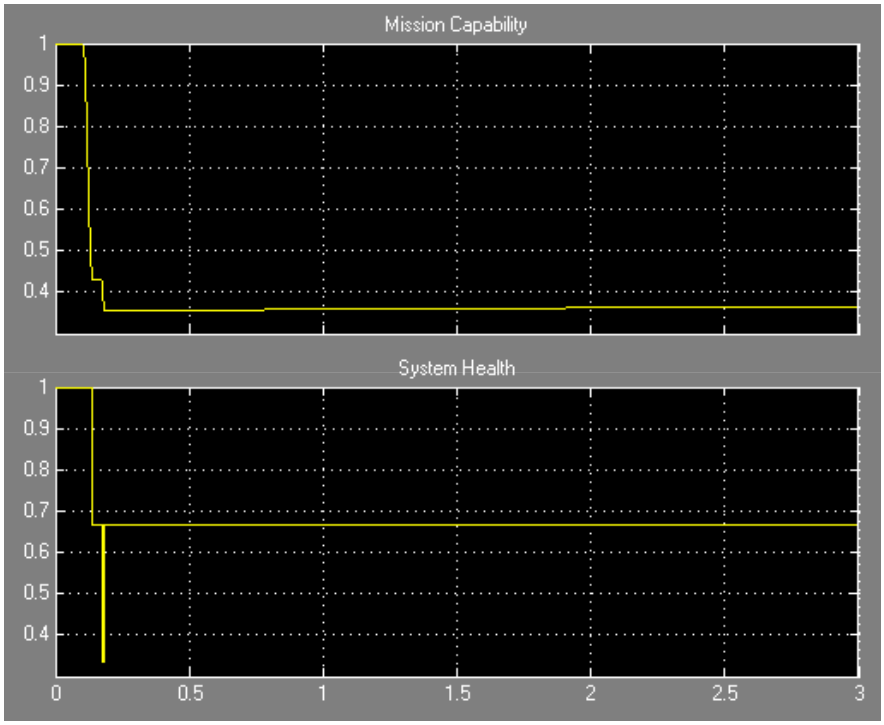


Figure 123: Time histories (in sec) of Mission Capability and System Health responses

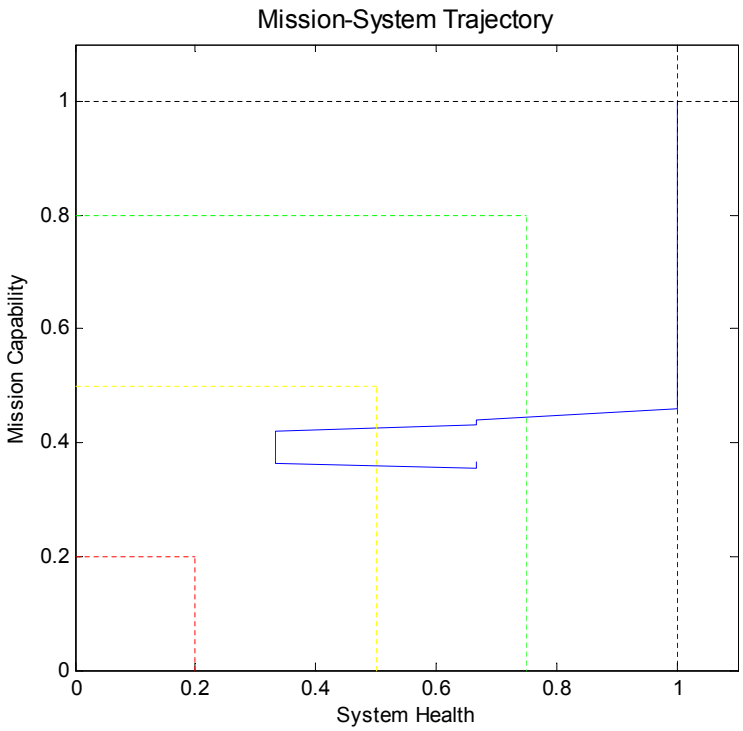


Figure 124: Mission Capability and System Health trajectory for a single mission and threat scenario

The Mission Capability $MC(t)$ is then defined as:

$$MC(t) = exp(-x_{max}(t)/L) \tag{74}$$

where L is a reference length. System health is defined as the current total stiffness $k(t)$ in comparison to initial total stiffness k_0. Namely, System Health $SH(t)$ is defined as:

$$SH(t) = k(t)/k_0 \tag{75}$$

A typical set of Mission Capability and System Health time history curves are presented in Figure 123. Both MC and SH are varying from 0 to 1, with 1 referring to the system's normal operating states. Based on the MC and SH time histories, the system's trajectory path for a particular mission and threat scenario can be obtained. An example is shown in Figure 124.

5.3 Resilience assessment for the baseline configuration

In accordance to the proposed technique, the resilience assessment on the system baseline entails the four analysis tasks listed earlier, namely survivability, life distribution, damage propagation, and resilience capacity analysis. The baseline configuration for the SMD system is defined according to parameter, and spring settings as explained in Tables 2 and 3. The particular study is concluded with the investigation for correlations between resilience capacities. With respect to the experimentation plan, the present section contains the results of Experiments 1.1, 1.2, and 1.3., which themselves have been formulated as responses to Hypotheses 2.2 and 2.3, and to Hypothesis 2.

5.3.1 Survivability calculations based on time durations

Life time analysis is a technique for collecting and performing statistical analysis of life duration measurements. Such techniques are used in medical and pharmaceutical research for analyzing and predicting the effects of a certain cure or medicine to patient. The measurements are presented in horizontal bar charts, or in needle charts in most cases, for emphasizing the durations of a patient's life time. An example of needle plot for life time analysis is shown in Figure 125, and represents life expectancies for the first 400 scenario cases.

Data from life time measurements could be used as the source of information for survivability calculations, based on the idea that survival is a function of a patient's life expectancy. The same notion is being brought in support of probabilistic calculations within the context of this research. With Figure 125 containing the SMD system's life expectancy results after experiencing certain disruptions, one could obtain a survivability plot with the proper calculations, similar to the one of Figure 126

For instance, according to Figure 126, the probability of achieving a life expectancy of equal or less than 0.5 sec is almost 0.78. A 2000 case Monte Carlo simulation

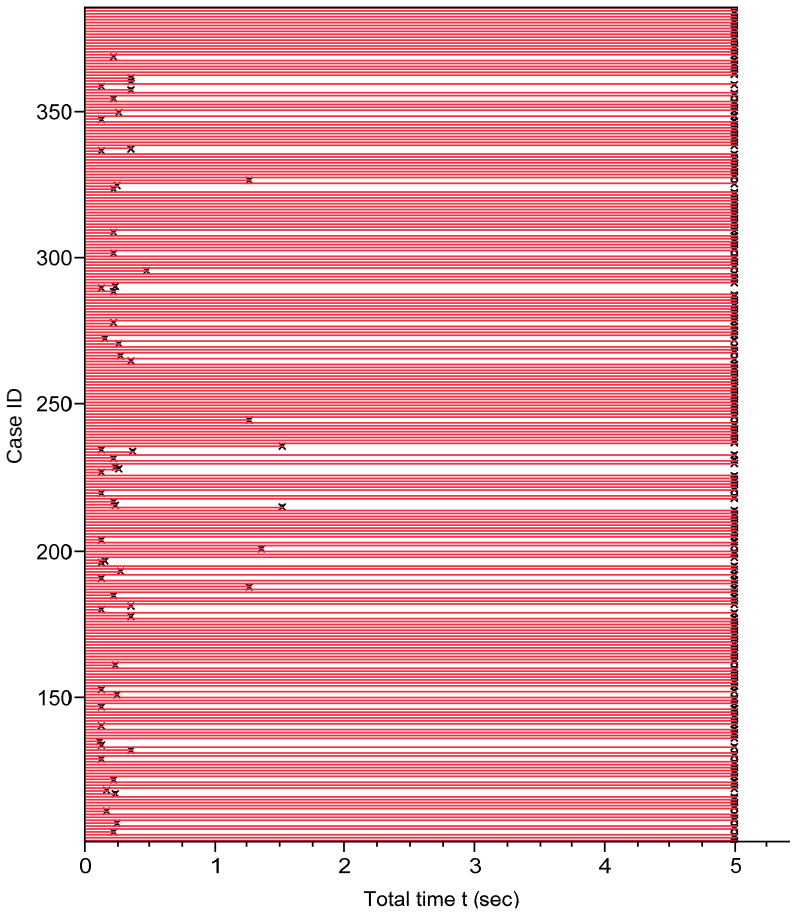


Figure 125: Life time analysis (*first 400 cases shown*)

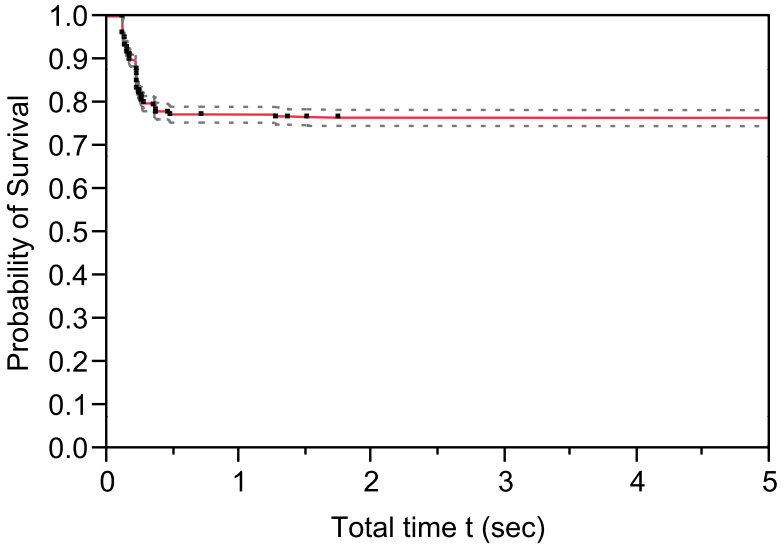


Figure 126: Probability distribution for system survival

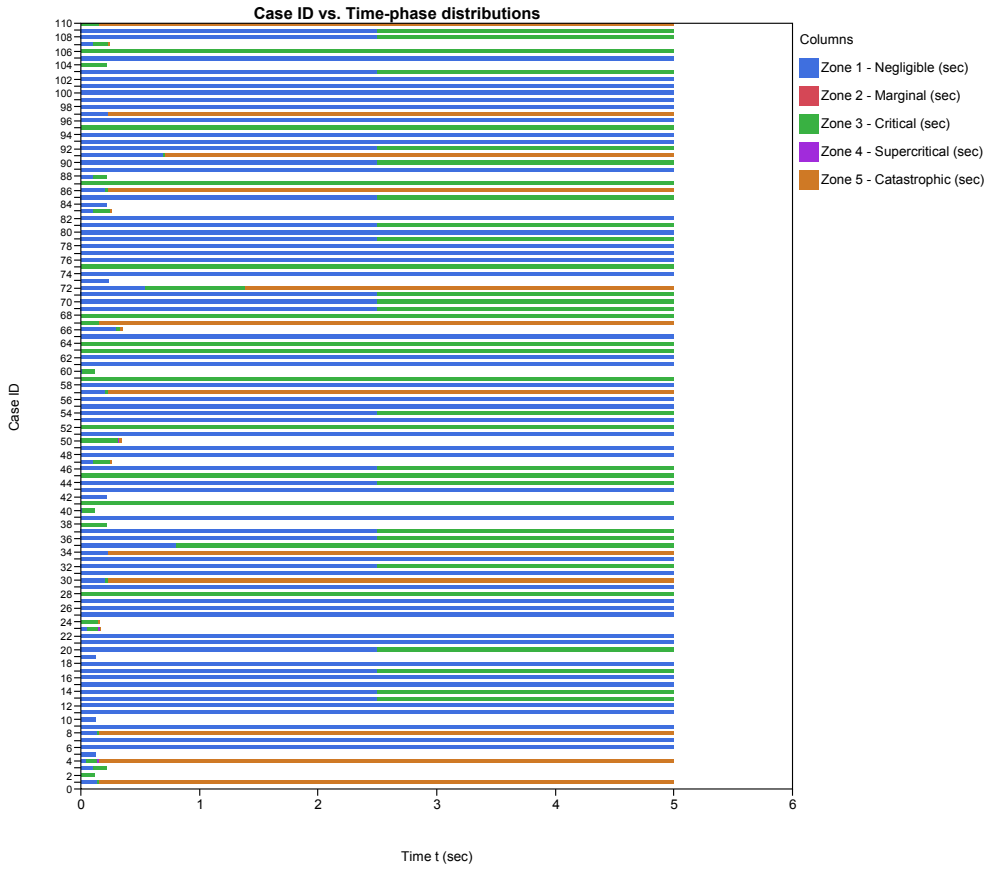


Figure 127: Life time per phase

procedure has been executed on the system baseline, which has a life expectancy of 3.8798 sec. When additional information on time breakdown is available, time life bars can contain distributions for the various epochs the system enters, during its normal operations. these epochs are application specific and are defined through system states, based on given thresholds. If similarly to safety engineering, one defines the critical thresholds for system operations, then its possible to allocate the portions of the total life time to epochs, where the system was operating within two consecutive thresholds. A representation of distributed life time measurements is given in Figure 127.

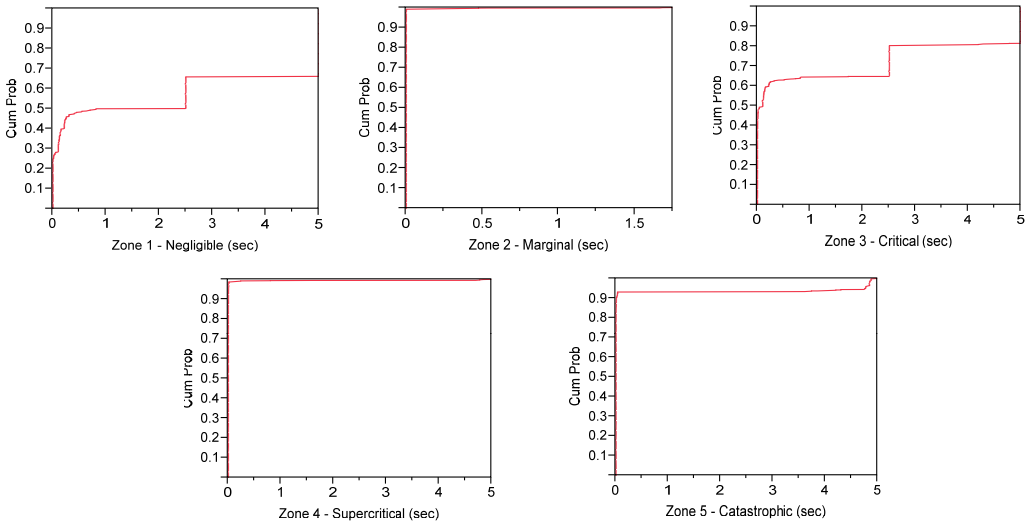


Figure 128: Time-phase CDF distributions for SMD model

5.3.2 Life time analysis

As part of the proposed assessment approach, life time measurements are used for probability estimates on how long would a certain system remain within two certain boundaries of operation, in a given threat environment. This is a useful enabler also for resilience-based design methods, as resilience of a system is pertinent to the time its remains active, and estimates of adaptability could be based on the time a system spends within two certain operating states. Figure 128 represents the CDF curves for time periods within certain critical operating zones. For the SMD system, it is observed that it did occupy most of the time either the low or critical degradation zone, with several cases reaching catastrophic failure under certain conditions. Intermediate zones, such as 2 or 4 where transitional zones, or regimes of low operational "width", thus the system almost occupies no time within them.

Hypothesis 2.2.2 states that resilient systems are more insensitive to uncertainty factors, with respect to their life time, and furthermore to their life time distribution. Figure 129 explains the phenomenon for the baseline, however, factors such as frequency, threat activity duration and the magnitude of the disturbance are the most

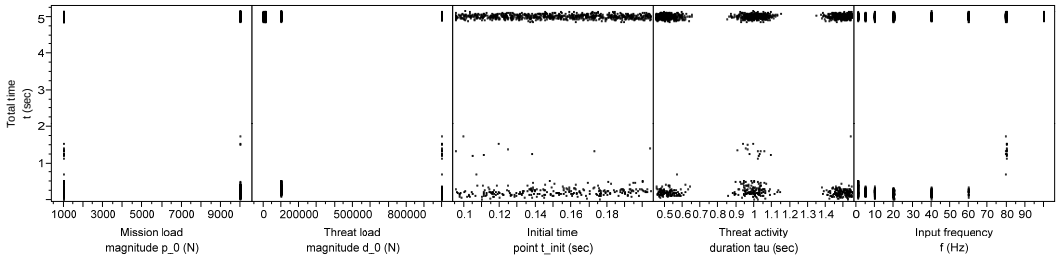


Figure 129: Effects of variable inputs to total survival time

significant contributors to the variability of total life time.

To expand on this observation, the correlation of time phase distributions against uncertainty, further supports the earlier hypothesis. The allocation of system response to a time zone is discrete, with certain levels of time periods observed for each zone. Variability in uncertainty does not affect the time period levels, except for input frequency and load magnitude. In support of the previous claim, Figure 130 contains the mapping of uncertainty to time phases for the baseline SMD configuration.

5.3.3 Damage Propagation

Damage estimation is another key measure for the support of system resilience assessment. Damage is observed through capability time histories, along with extreme values for system degradation and the degradation rates. It is interesting to investigate the impact of uncertainty on mission capability and observe any modes of damage through the variation of the performance time histories. Based on the MC histories for the SMD model, the damage propagation index (DPI) is defined as a cumulative estimate of damage induced degradation on the system over the system's life time. As Figure 131 suggests, the DPI varies with uncertainty, and does significantly depend on the frequency of the input signal. higher DPI indices are observed in the region of all values of natural frequency that the system is characterized. Load and input duration also affect the DPI, but with less impact.

Equivalent to the DPI is the DPR which is the damage propagation rate, and is

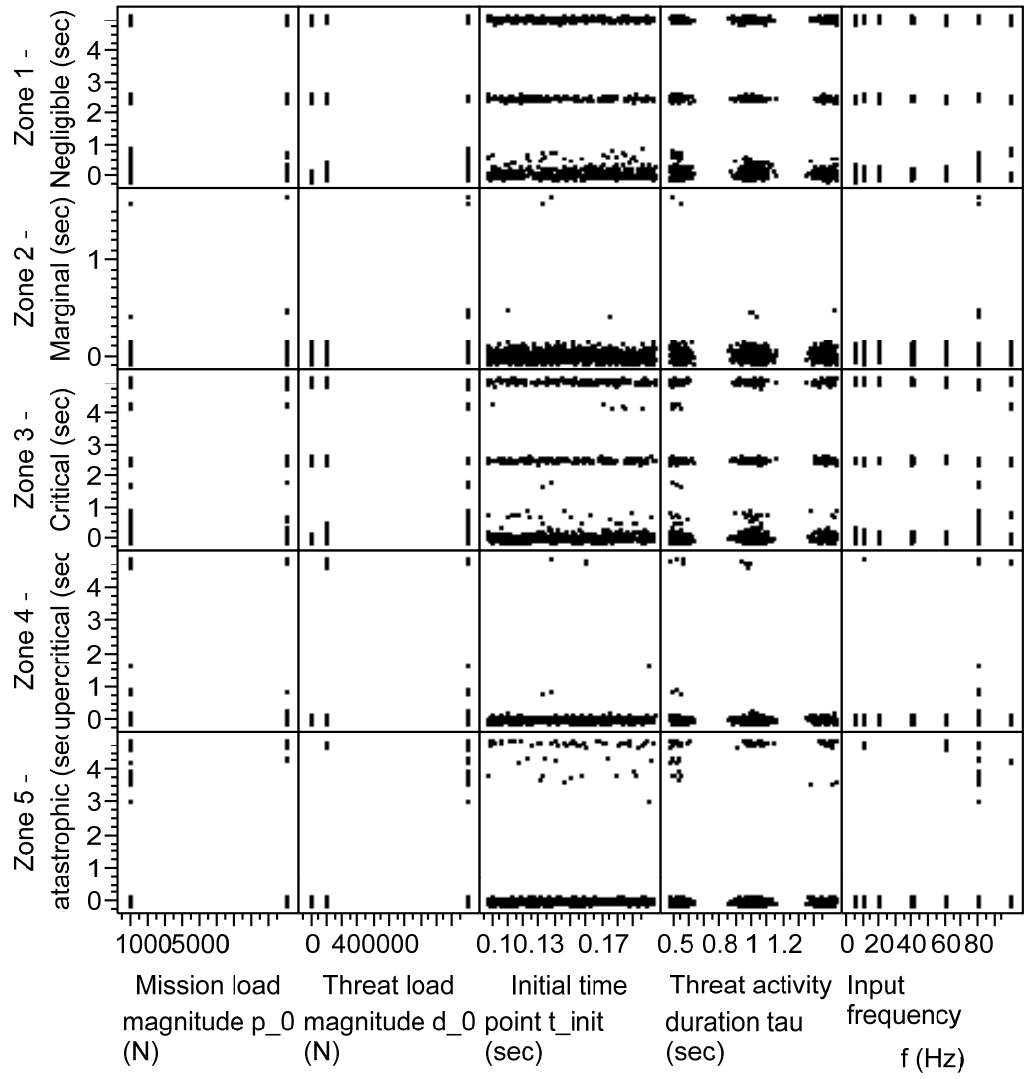


Figure 130: Time-phase distribution mapping to uncertainty

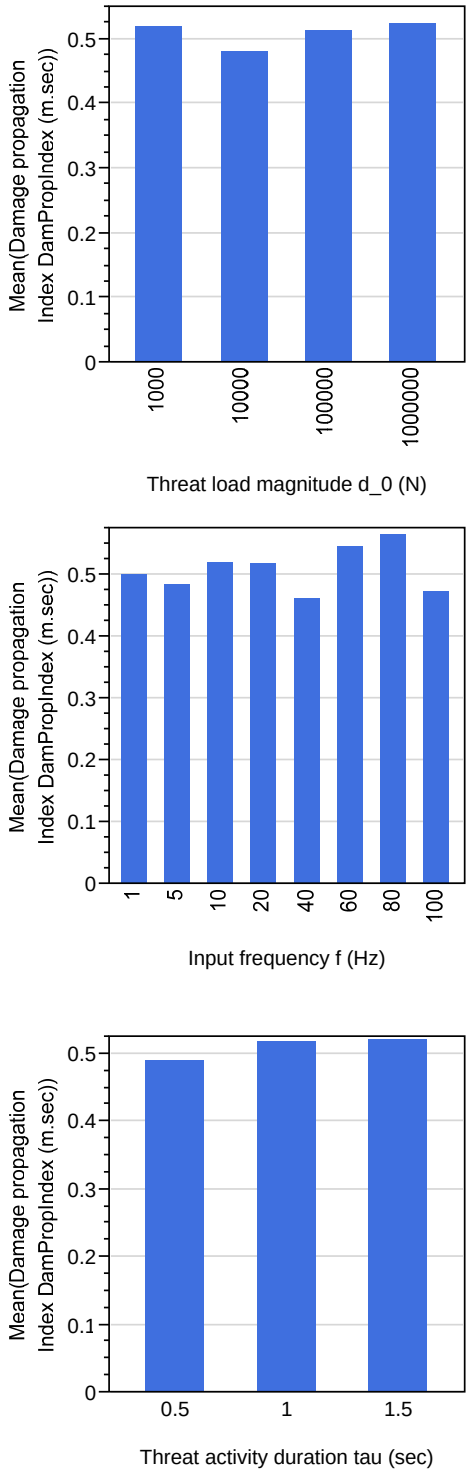


Figure 131: Damage propagation index (DPI) variation to uncertainty factors

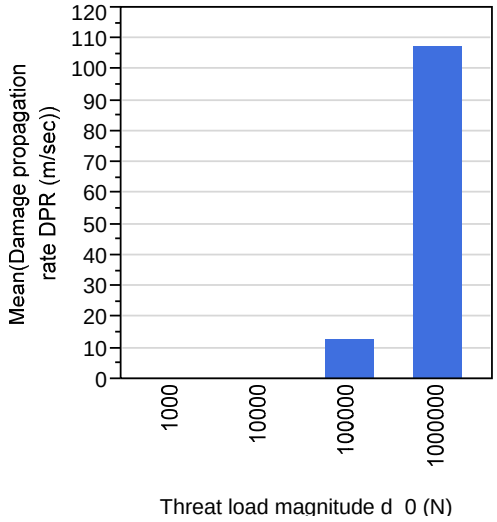
a measure of the rate of change of system degradation, for the time that the system actually degrades over a threat. Figure 132 also indicates the effects of the frequency and the higher variability in the range of the system's natural frequencies (10-50 Hz).

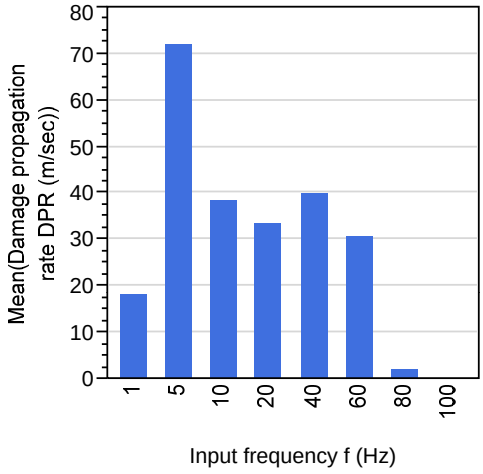
Last, a maximum point for the degradation due to damage can be defined as the maximum damage point. It is the point of an MC curve, where the effects of recovery start manifesting themselves. This point is also a measure of a system's static robustness. Figure 133 explains the impact of threat amplitude and input frequency on the maximum damage point. As the system operates close to its natural frequency, the damage propagation is increasing, as it depends on the displacement of the SMD oscillation. Regarding the threat magnitude, the smaller maximum damage stands out as an oddity for higher values. This could be possible for systems that eventually collapse, with this damage extent being the maximum damage observed before the system entirely collapses.

5.3.4 Analysis of resilience capacities

As Hypothesis 2.2 has been addressed in the earlier section, Hypothesis 2.3 concerns the association of the resilience capacities to the uncertainty factors. It would be interesting to see for instance, how input frequency affects the resilience capacities, since it does influence survivability and damage related measures, as it has been previously demonstrated. Starting with the "restore" capacity, Figures 134, 135, and 136 show the variation of the recovery rate, time, the maximum degradation, the restoration offset, and the health ratio SH.

The activity time of the disturbance against the system has minimum impact on the restore function components. Indeed, resilient systems must always contain the readiness to respond to changing conditions, regardless of the occurrence time and duration of the input. Frequency does affect the five response metrics, but not as explicitly as for system response metrics, such as displacement, or mass acceleration.





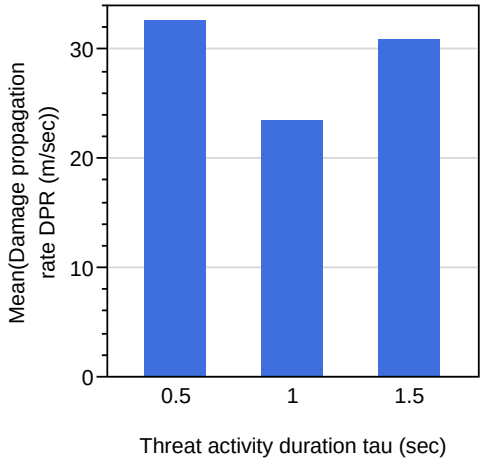


Figure 132: Damage propagation rate (DPR) variation to uncertainty factors

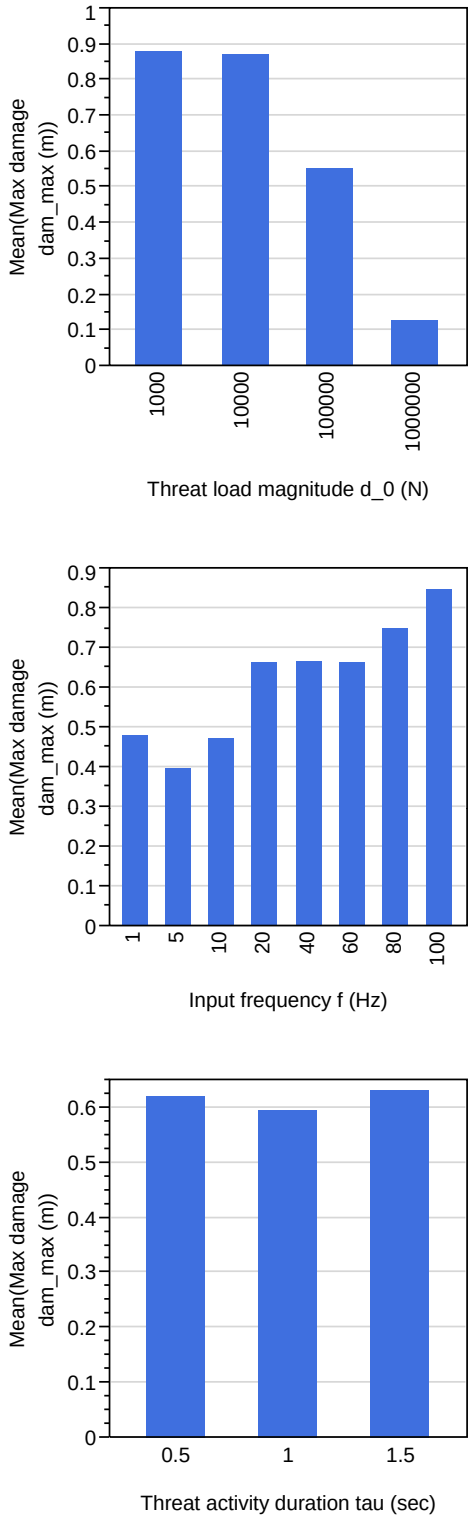


Figure 133: Maximum damage variation to uncertainty factors

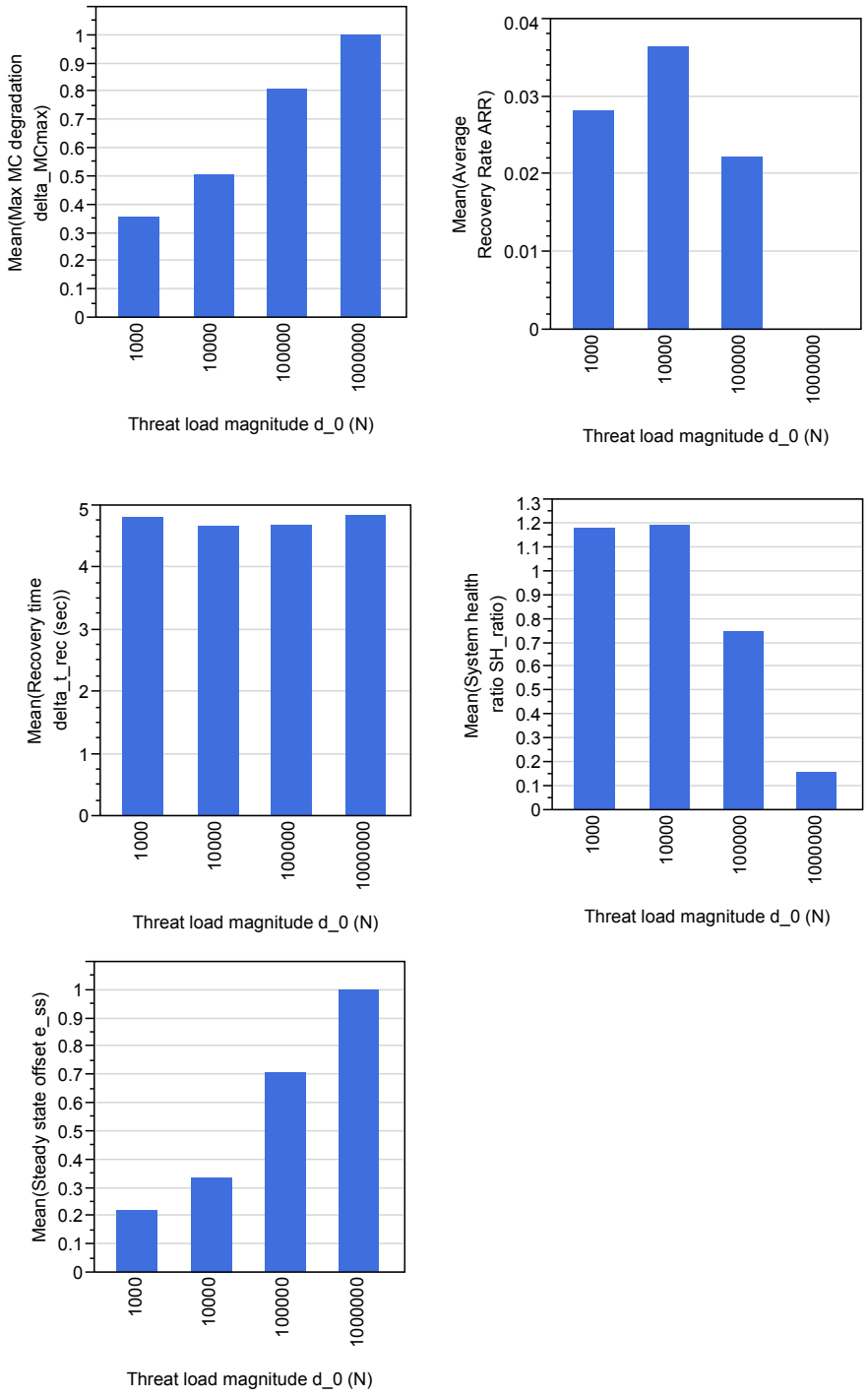


Figure 134: Uncertainty effects of disturbance magnitude on "restore" capacity

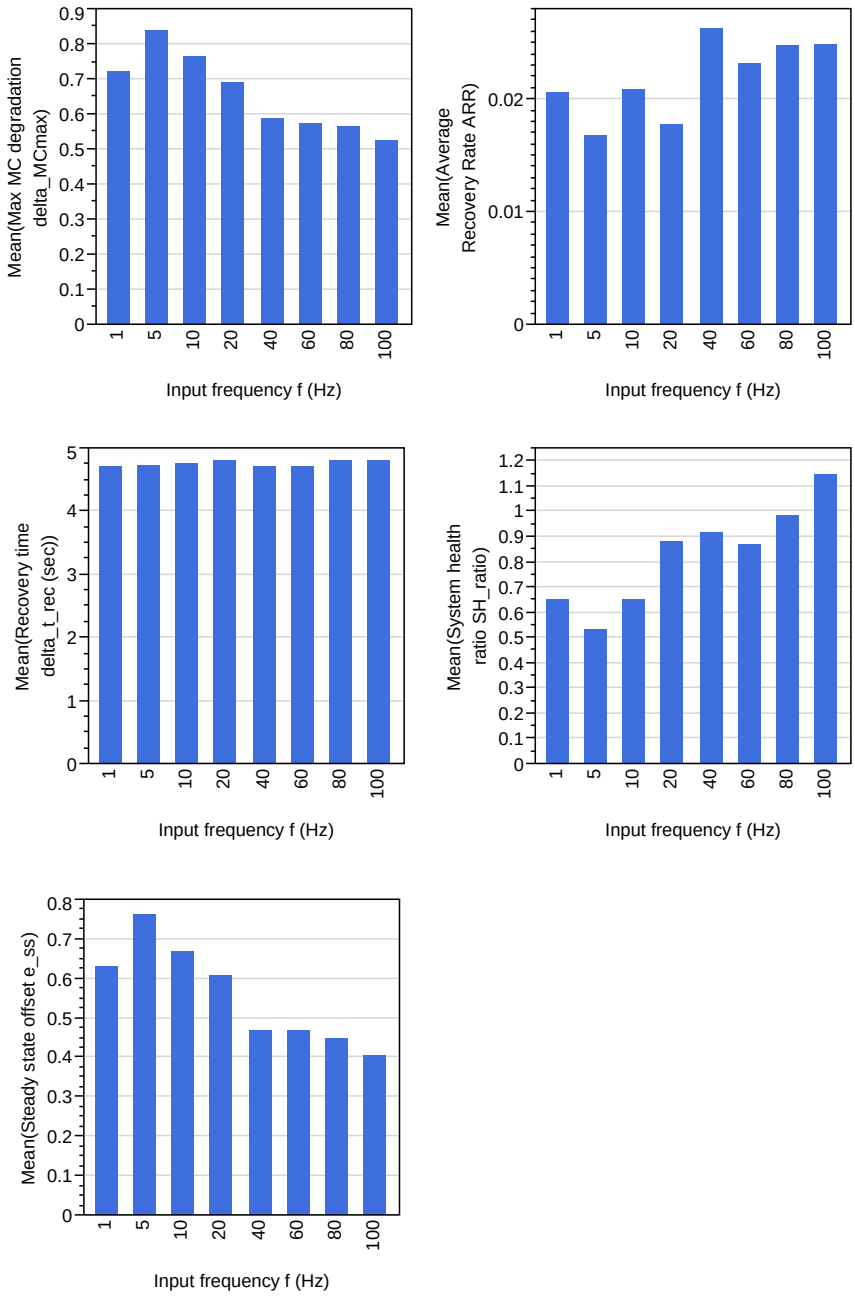


Figure 135: Uncertainty effects of frequency on "restore" capacity

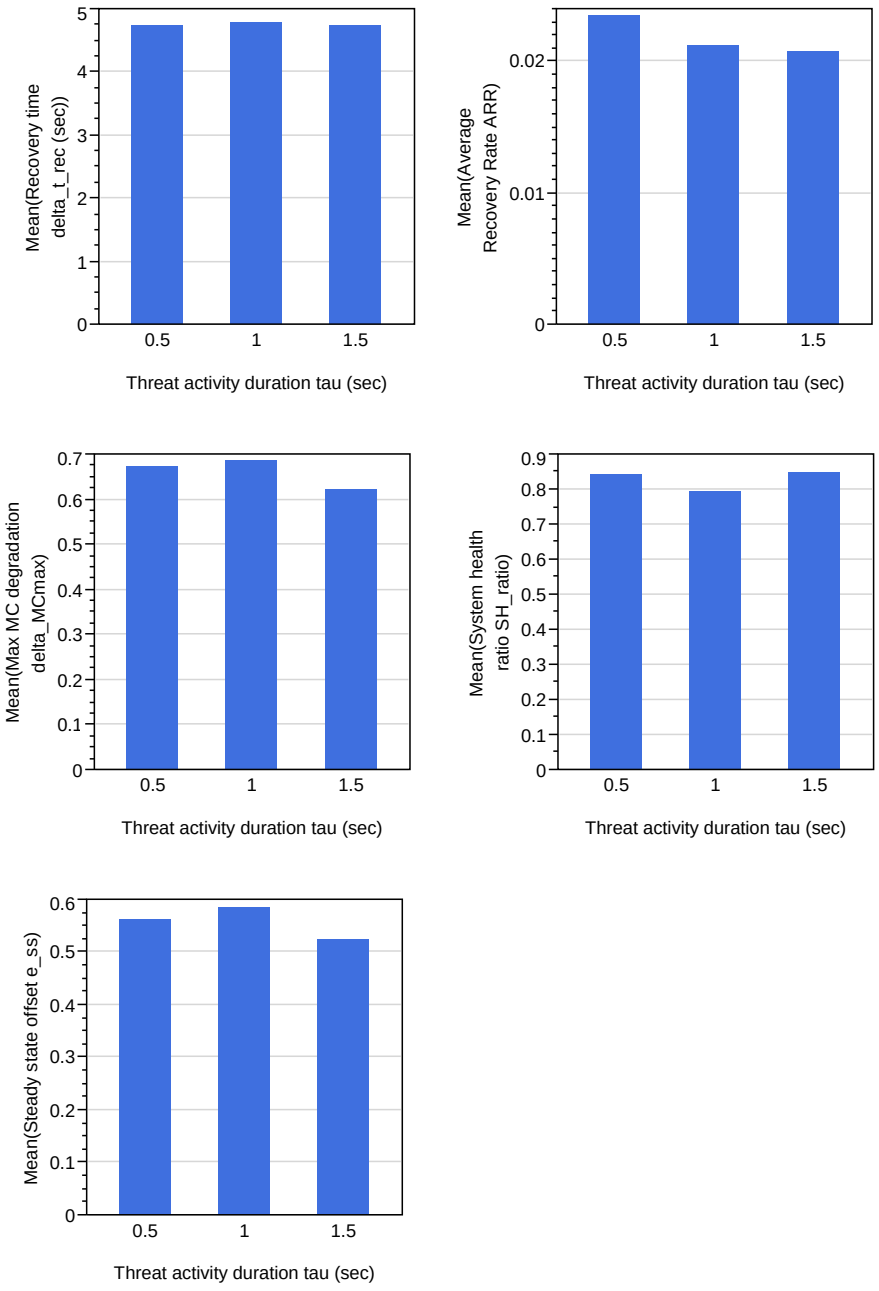


Figure 136: Uncertainty effects of duration on "restore" capacity

The magnitude of the disturbance input however, does have a significant impact on the health status. As a result, input signal frequency, along with the magnitude of the disturbance, drive the characteristics of the system recovery process.

A system's absorbing capacity is closer to system robustness, as it has been discussed in earlier chapter. In the context of the resilience framework, the system's absorb capacity depends on its ability to persist against the threat effects, either by neutralizing their impact, or actively fighting against a threat. To quantify the capacity of system to perform these action, the time-averaged performance degradation is defined for system. Alternatively, there is the time-weighted averaged performance degradation, which brings the aspect of timing into the process.

To illustrate the contrast between these two metrics, Figure 137 presents the two averaged system performance degradation measures, for the same scenarios and same impact of uncertainty. Except for the impact of uncertainty of the performance degradation itself, it is illustrated how the time-weighted metric emphasizes the effect of time. Input signal close to the system's natural history, result in a more complex behavior, which is not always predictable, and this seems to be captured by the time-weighted metric, thus making it more suitable for time sensitive systems. In the remainder of this study however, the non time-weighted metric is used instead.

As an extension of the time-averaged metrics, the disturbance to threat D/T ratio is defined, to bring the strength of the threat disturbance into effect. It is equivalent to a signal-to-noise ratio, but it seeks to compare the impact that a disturbance has on system performance, to the strength, or magnitude of the disturbance. Figure 138 demonstrates the effects of increasing disturbance duration, input frequency and load magnitude of D/T. The ratio is increasing with the duration and the magnitude, yet it appears to be almost independent of the input frequency.

Last, the system's capacity to adapt to change is being brought into focus. The system's ability to adapt to changing environmental and mission related conditions,

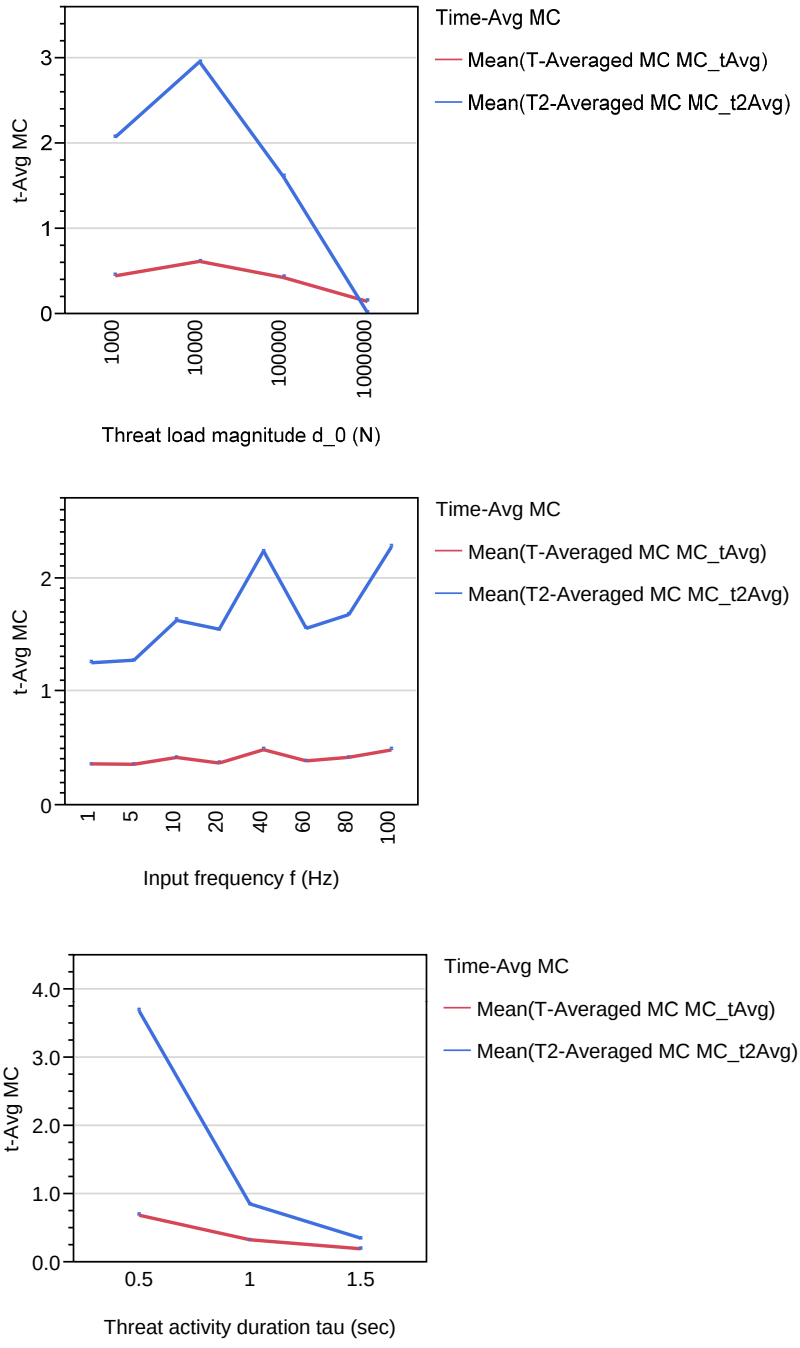
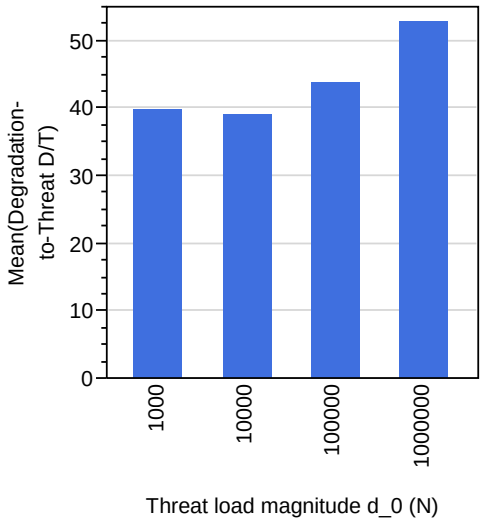
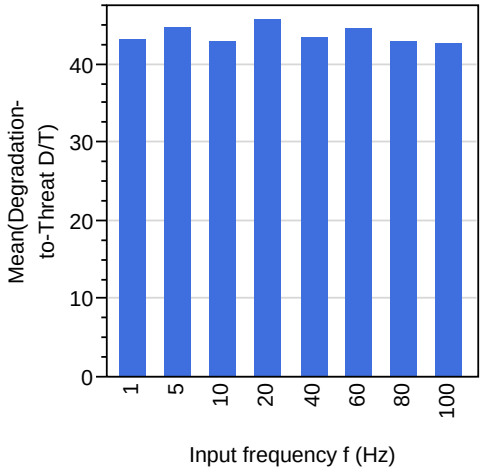


Figure 137: Uncertainty effects on "absorb" capacity (Time-averaged MC)





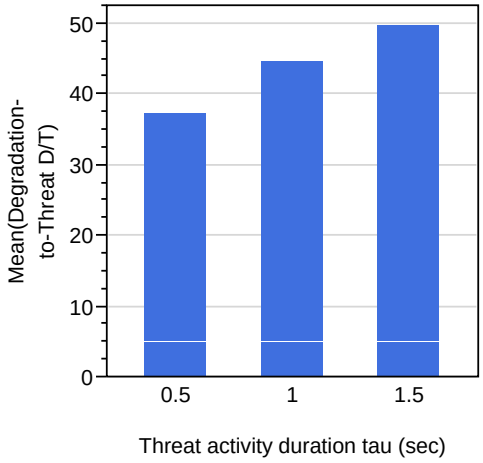
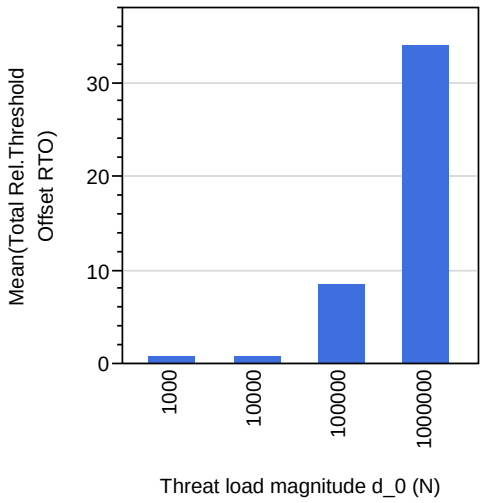
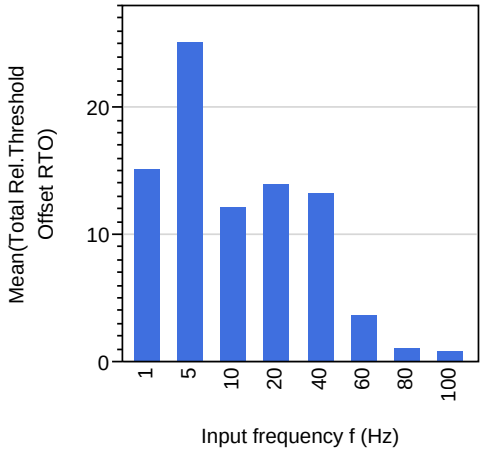


Figure 138: Uncertainty effects on "absorb" capacity (Degradation-to-threat D/T ratio)





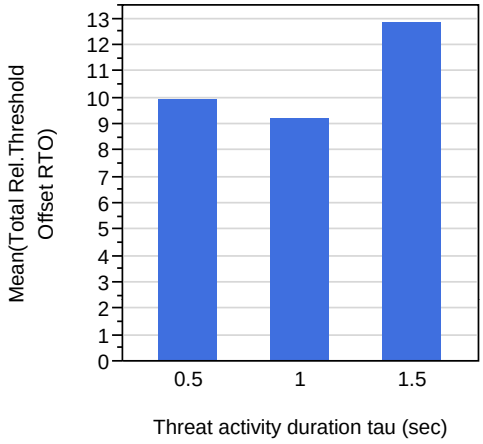


Figure 139: Uncertainty effects on "adapt" capacity (Relative threshold offset RTO)

depends on its ability to sense the threat impact on itself, to see how it may be possible to avoid the threat impact, and if this is not quite possible, to explore options on how it can accommodate itself to changing conditions. The relative threshold offset RTO for the MC time histories is a metric that describes the performance deviation from a critical threshold, and accumulated over the time period of the system's activity. It is an estimate of how far system performance could deviate, if it is desired that for a stable response it must stay within a certain distance from a particular critical threshold.

Figure 139 hints that the magnitude of disturbance increases the RTO, thus the system is prone to exceed the boundaries of its normal operating condition. In contrast, an adaptive system response would activate the mechanisms of maintaining its performance position over time, thus the RTO would have remained low. Another important fact is the impact of frequency. If the input signal is of a frequency in the neighborhood of the system's instantaneous natural frequency, resonance effects could take place and force the system to deviate from its normal operating band. If it's not adaptive, the system would be more vulnerable to such effects. As the frequency steps into higher values, away from the system's natural frequency, maintaining performance is improved. Last, the activity duration, hints on a turning point in RTO with longer disturbances. As the optimum response is in the middle, short or long term effect appear t have equivalent impact on system adaptability.

The end of this section has marked a collection of experimental findings, in support of Hypothesis 2.3.1, which claims that resilient system vary their capacities of being adaptive and robust, with the presence of uncertainty factors. This is a natural outcome, that is pertinent to the "adapt" and "absorb" functions, which require for the system to sense and assess its environment, in order for it to evolve through the changing conditions.

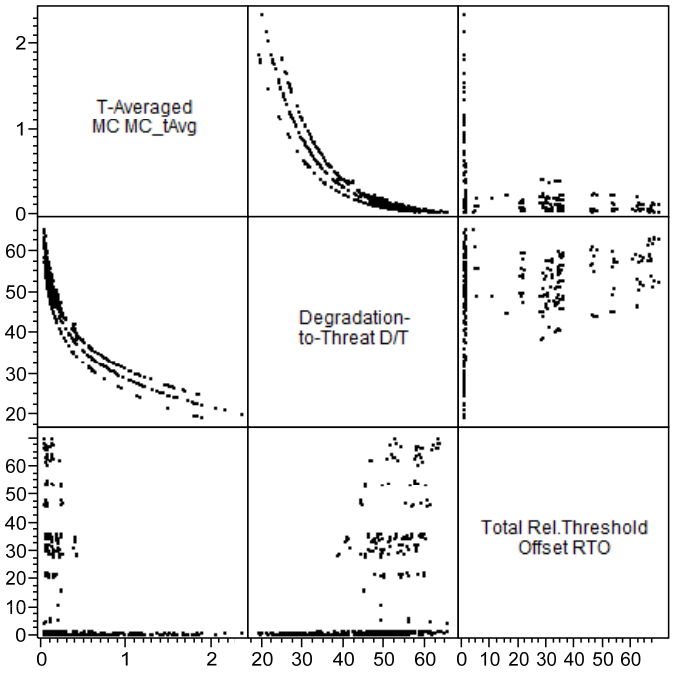


Figure 140: Correlation matrix for adaptivity and robustness metrics

5.3.5 Correlation and sensitivity analysis for resilience capacities

After discussing the implications of investigating the variation of resilience capacities to changing uncertainty factors, one would wonder whether the metrics that express the resilience capacities are varying in correlation to each other. This is quite possible, as many of these metrics are based on mission capability and system health calculations. Despite the fact that they seek to address a different aspect of the problem, they cold be correlated in certain ways.

Correlation studies for resilience metrics is necessary, in order to ensure that the same phenomena, described by two different metrics are identified. In Figure 140, a correlation matrix for the adaptive and absorptive resilience capacities is presented. It quickly becomes obvious that the time averaged performance degradation is correlated to the D/T ratio, with a factor of 0.9549. Far less correlated the former, is the adaptability measure RTO, which appears to be practically independent of the

other robustness measures. This is a key observation on robustness and adaptivity, as they are both supporting concepts to resilience, yet they serve different objectives, with different internal mechanisms. Last, in the prospect of a resilience-based design method, the two capacities could initiate design space exploration studies, while allowing the designer to optimize for cost, when the capacities are accompanied with technology solutions for their implementation.

5.4 Trade studies for resilience enhancement strategies

As part of investigating Hypothesis 3, the planned Experiment 1.4, looks into identifying and discussing the effects of robust system solutions to the resilience capacities. Experiment 1.5 repeats the same analysis process, but with the use of alternative control strategies and configurations. On the basis of adaptability and robustness being fairly independent, two different paths have been follows. Architecture modifications in the form of redundant systems, effective, high strength materials, all result in a more robust system, in the sense that they provide the mechanisms for the system to naturally absorb the effects of unexpected disturbances. Control strategies and architectures, are enablers of more adaptive systems. They provide the ability for the system to monitor and record its surroundings, to evaluate the situation and react to a disturbance. Despite the fact that there are clear lines between robustness and adaptability, this should not imply that a robust system cannot be adaptive to change to some extent, or vice versa.

5.4.1 Enhancements for system robustness

As the purpose of the canonical problem is to be the platform for the development of the assessment technique, it is acceptable to model notional robust system solutions, through incorporating models of their effective mechanisms. For instance, robustness of a SMD system is not only improved through the number of the main, or redundant springs, but also through damping, which provides for another mechanism for the

system to be able to absorb the effects of a force disturbance.

For experiment 1.4 therefore, a Monte Carlo simulation is performed with 2000 cases, under three different damping settings. For the baseline, the damping ratio is $\zeta = 0.02$, while the other two settings are for $\zeta = 0.01$ and 0.04. The analysis procedure, follows the steps as listed in Figure 117. The first responses of interest, are the life time distributions. Figure 141 presents the system's time life, with uncertainty factors, and for three levels of damping ratio values. As discovered earlier, the impact of frequency and the disturbance magnitude of the system, is more significant than duration of the input, or its occurrence time point. However, the middle setting of ζ appears to be almost independent of the two factors. As robustness reflects the insensitivity of a system to uncertainty, this setting would be a logical design choice. Regarding the trends, larger input forces reduce the life time, while lower frequencies, closer to the system's natural frequency, reduce the life expectancy, as resonance effects appear and result in earlier catastrophic effects.

Moving into damage analysis, the observed degradation times also give glimpse of more stable configuration, for the one with damping $\zeta = 0.02$. Higher damping results into faster degradation, as is the case for lower input force magnitudes. In terms of input frequency however, there is greater variability and a low point is observed close to the system's natural frequency. The offset from the original performance value is presented in Figure 143, while Figure 144 describes the effects of damping on the recovery time. Damping does not have an impact on recovery time, as it prevents degradation, and does not actively enhance recovery.

Estimations for resilience capacity on the "absorb" function are presented by Figures 145 and 146. The time-averaged MC degradation is sensitive to frequency input change, with the outer settings of the ζ range to have the system's degradation fluctuate more than the middle setting of $\zeta = 0.02$. Confirming earlier observations on the stability of the 0.02 damping setting, the change of input duration and magnitude

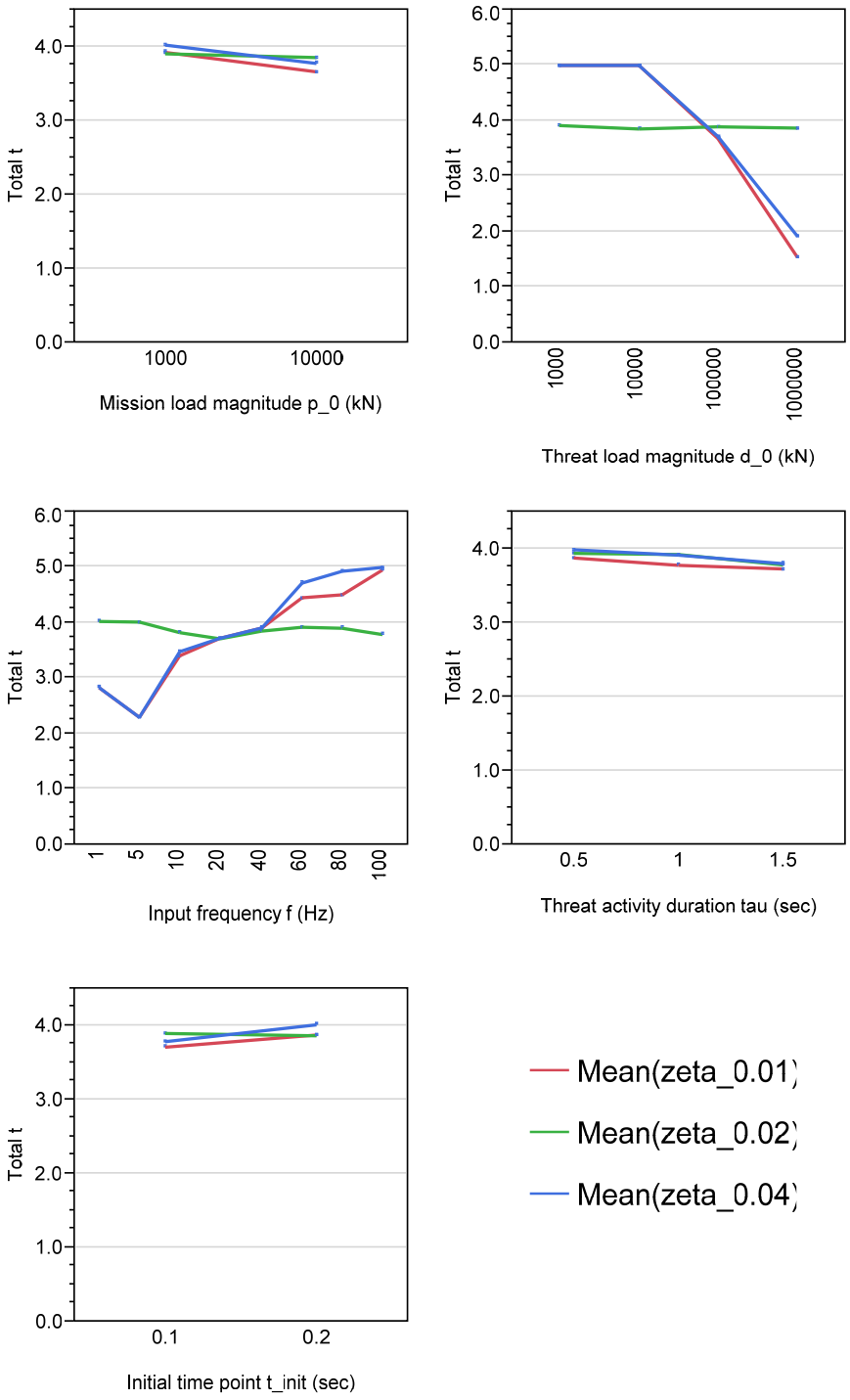


Figure 141: Variation in survival times with damping ratio

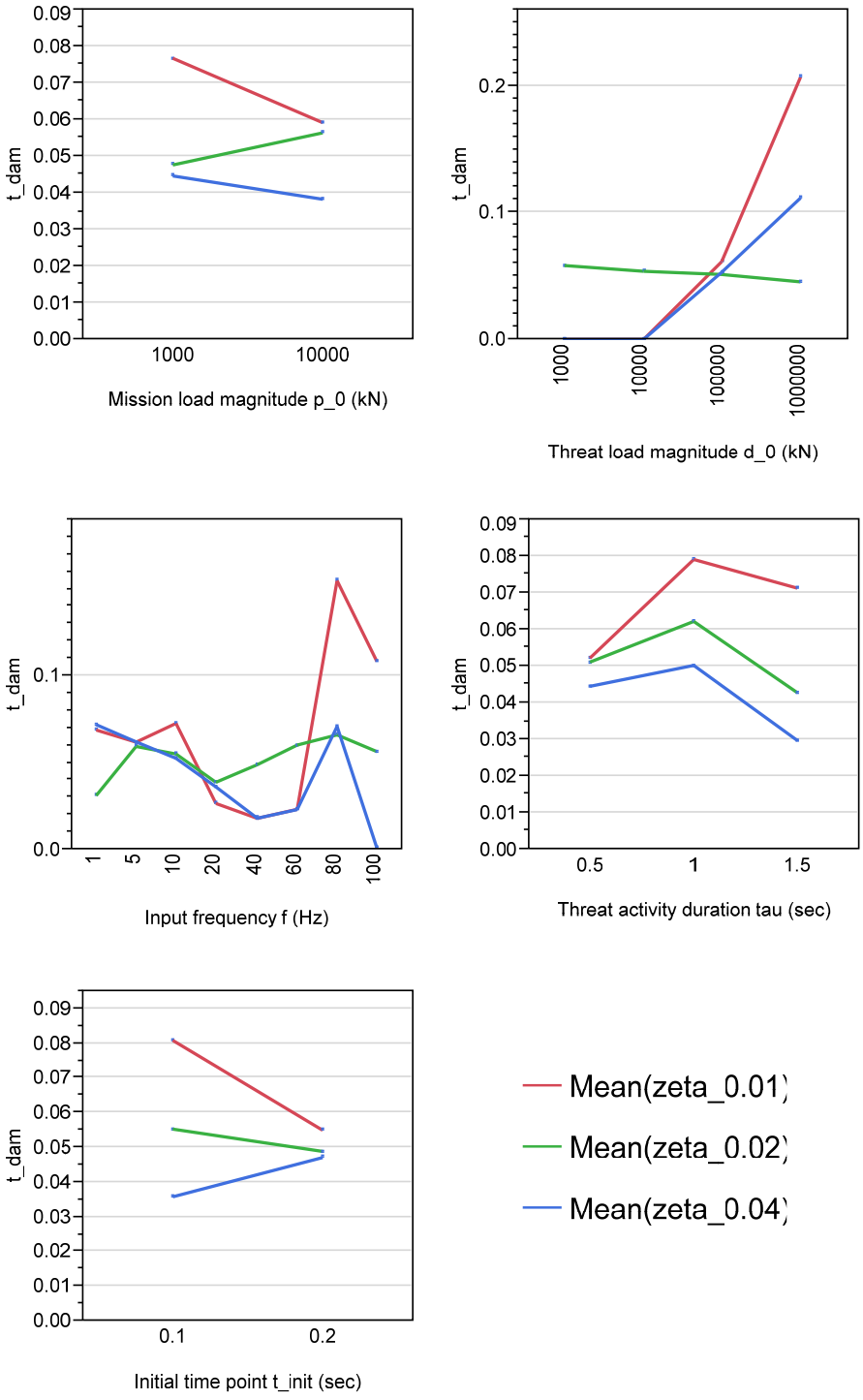


Figure 142: Degradation time period with damping ratio

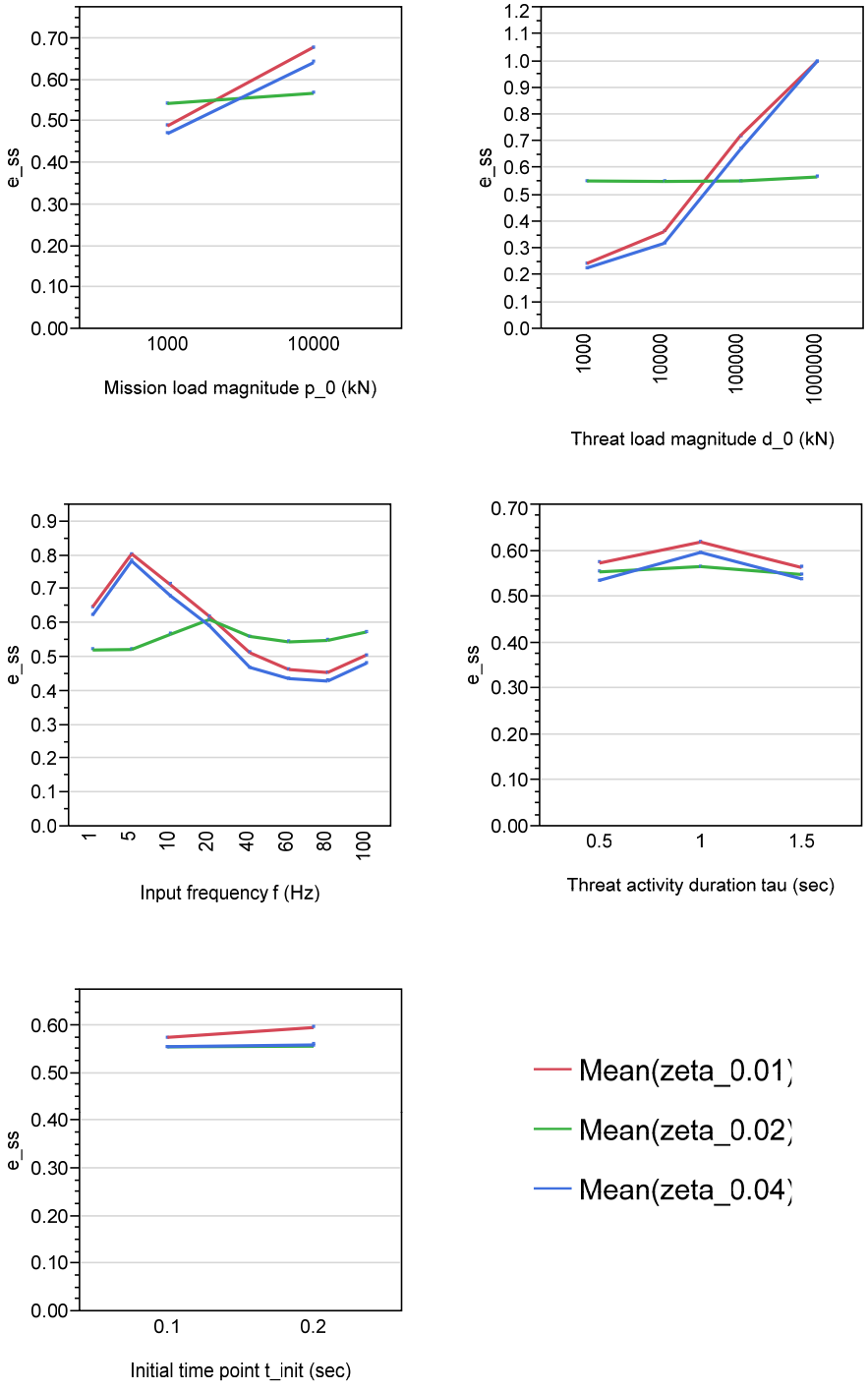


Figure 143: Recovery offset with varying damping ratio

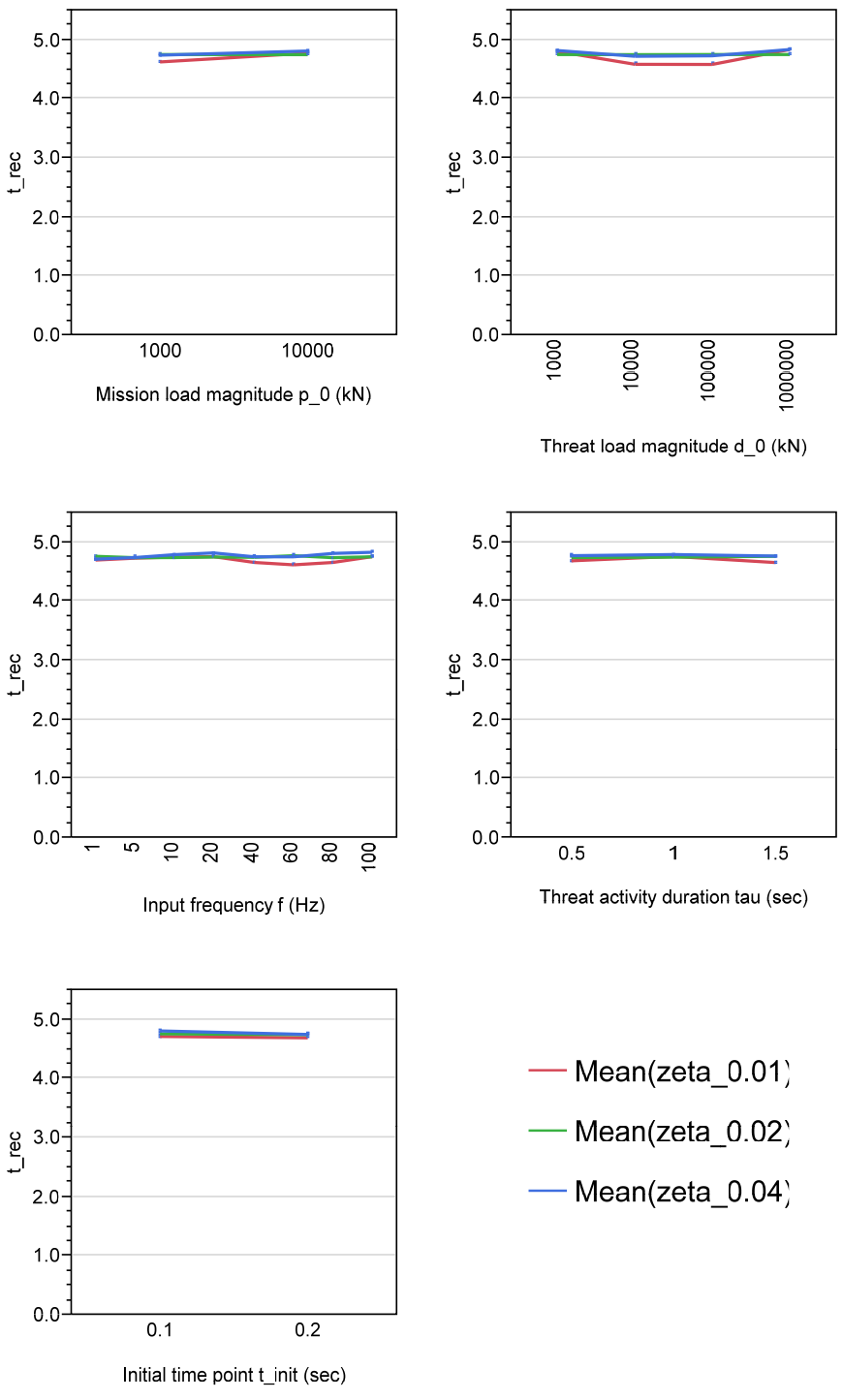


Figure 144: Recovery time with varying damping ratio

result in a more stable time-averaged performance degradation. Despite the fluctuations on the time-averaged MC degradation, the degradation-to-threat ratio results to more stable responses for all three damping settings. The uncertainty variation on threat activity duration, load magnitude further confirms the insensitivity of the 0.02 setting to external change. Thus, from a robustness point of view, technologies or solutions that would bring the damping ratio level to 0.02 would allow the system to better "absorb" external change, thus making it more resilient through being robust.

The "adapt" capacity estimates are provided by the RTO metric and the responses to the varying three major uncertainty input factors is presented in Figure 147. Larger values of RTO could either imply a large offset from a critical threshold, which is a desired characteristic, or a large offset from less critical threshold, that could hint that the system has reached a critical threshold. For different applications, the partial RTO estimates indicate the actual offset from thresholds, and they are key for defining the most adaptive response, with respect to them.

5.4.2 Reconfiguration strategy tradeoffs

Experiment 1.5 is a a comparative study, which requires the resilience assessment of alternative control strategies and configurations, and then compares the responses, in a n effort to identify the most stable, robust and adaptive solution, which according to the resilience definition, can be accepted as the more resilient configuration. The alternative control strategies differ in terms of what and how many springs are activated by the rule based controller.

A strategy forms the rules for the controller's action, and it receives feedback from total system stiffness measurements. In other words, when one or more springs reach their limits and eventually break, the loss in stiffness is logged by the health monitoring system and triggers the commands which decides what redundant spring to activate, in order to compensate for the lost stiffness. The first two strategies

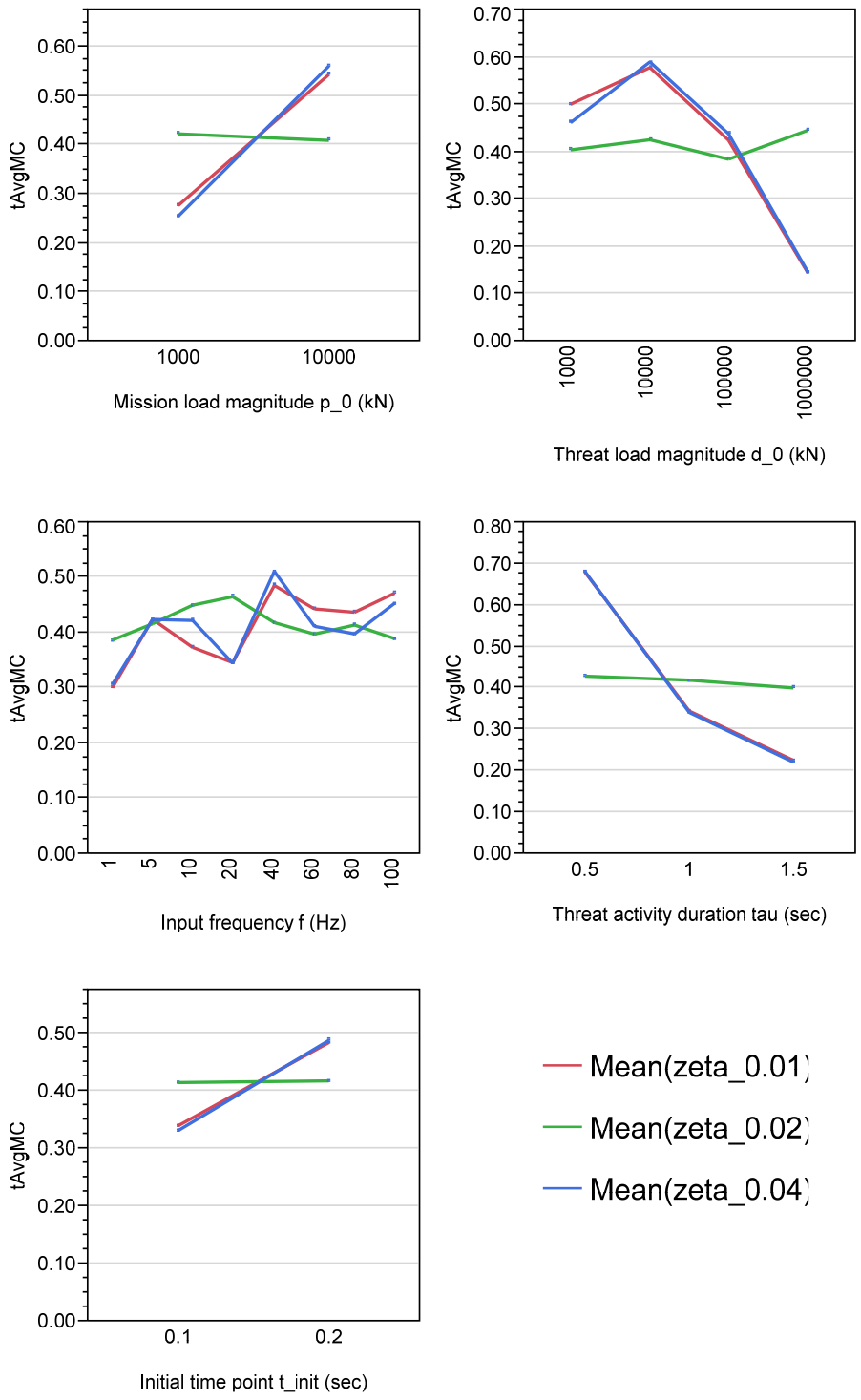


Figure 145: Time-averaged performance degradation with damping ratio

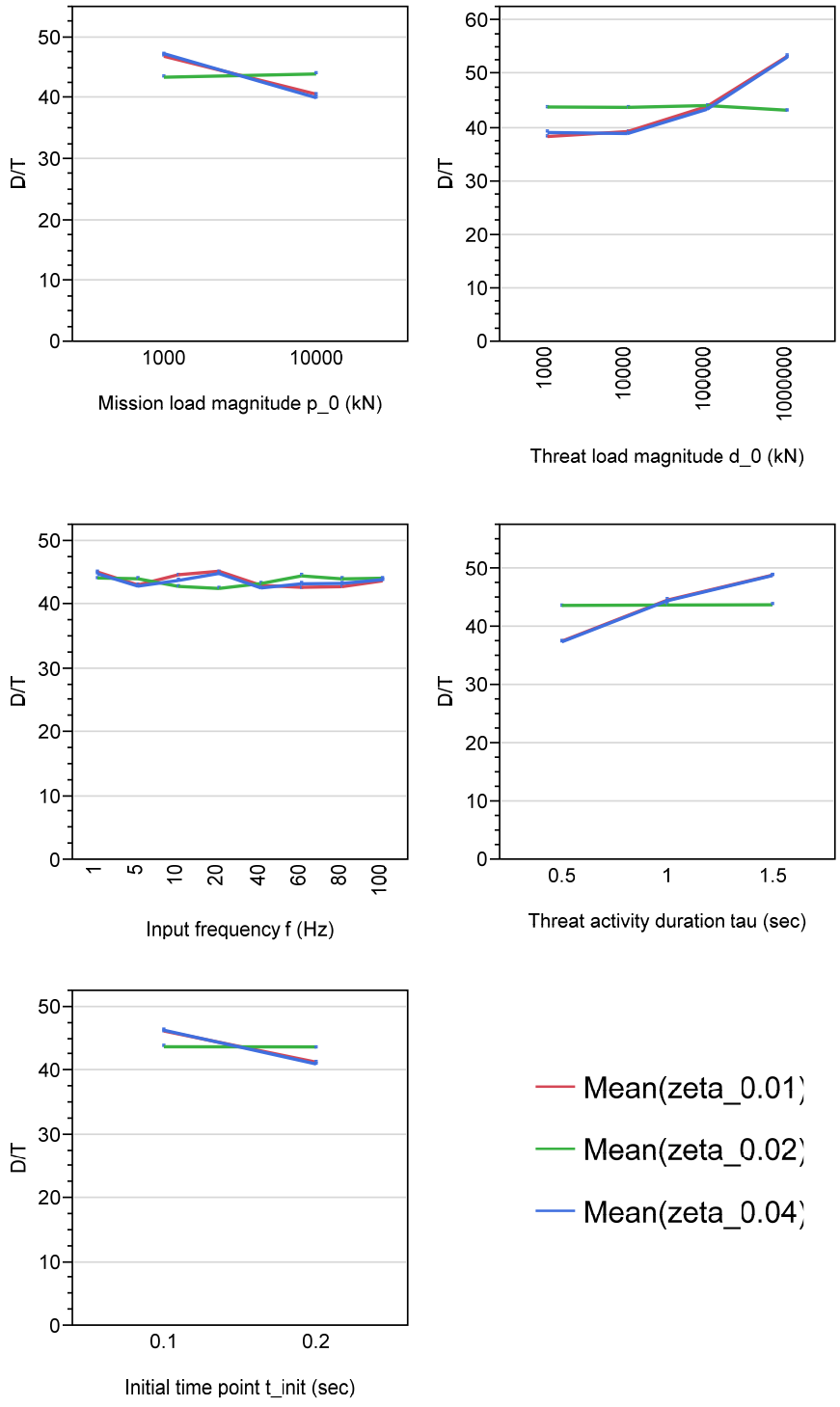


Figure 146: Degradation-to-threat ratio with damping ratio

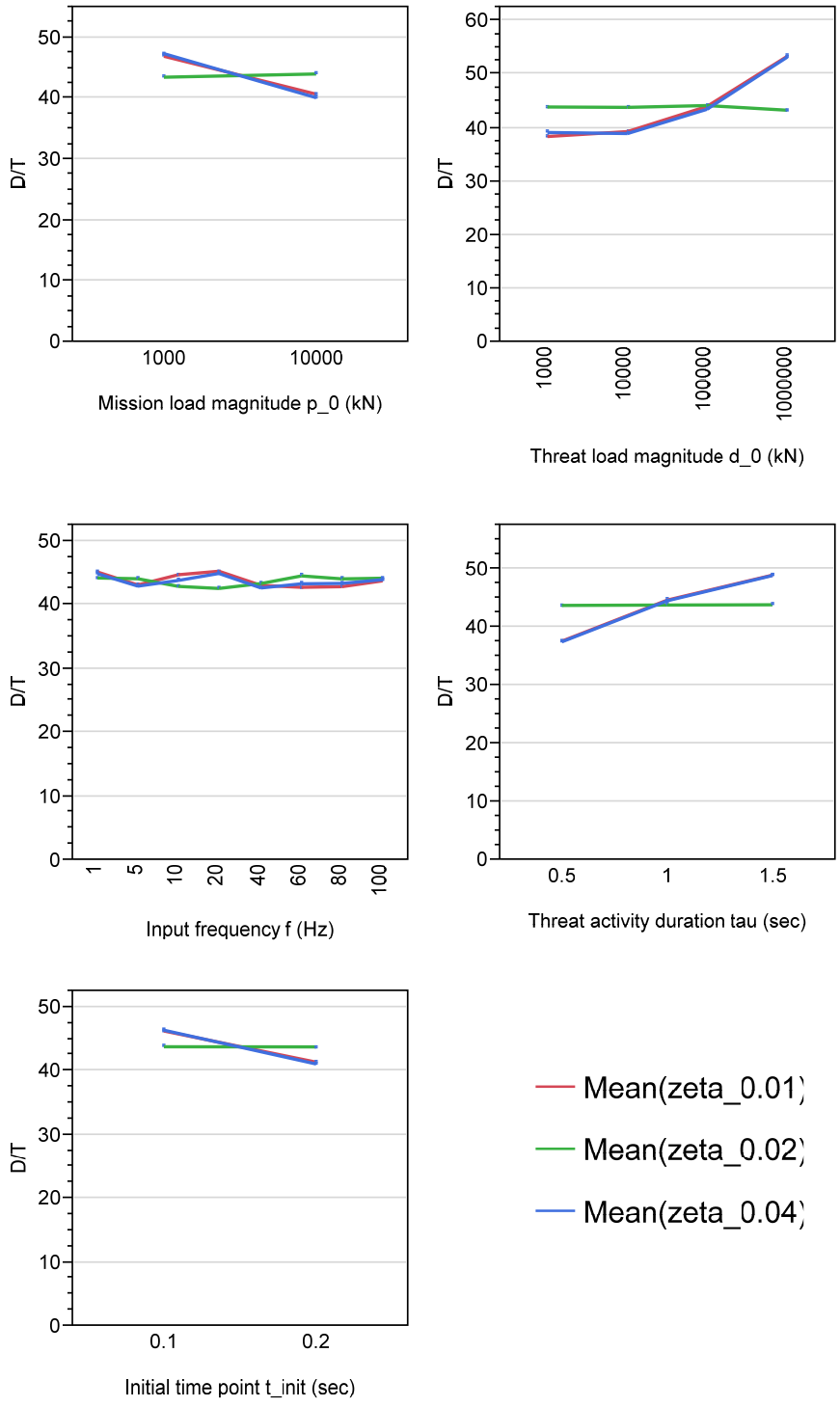


Figure 147: Relative total threshold offset RTO with damping ratio

(CTRL0, CTRL1) are quite conservative in usage of additional resources, thus allowing the system to get closer to the critical threshold, before they commit to full activation of additional stiffness. The two latter (CTRL3, CTRL4) are more generous at earlier thresholds, attempting to ensure the system always carries adequate stiffness. Strategy CTRL3, is an intermediate approach that brings a more balanced stiffness activation strategy.

Starting with the trends in survival time, Figure 148 presents the time until mission end or earlier collapse for all 5 control strategies, under the presence of uncertainty, in the form of four varying external factors. These are the load magnitude, and frequency, given that the load is playing the role for the external threat, along with variation of the starting time instant and its activity duration. From a general overview standpoint, it is strategies CTRL1 and CTRL2 that demonstrate better stability and insensitivity to the changing uncertainty factors. However, for strategies at the extremes of the alternatives range, maintain a better survival time for the lower part of the disturbance input range.

In terms of frequency, there is a larger deviation in behavior among the control strategies, yet there is an overlap of all alternatives observed for the range of 20-40 Hz. Except for the more robust CTRL1, and CTRL2, the other strategies, ensure better survivability for higher frequencies, than for lower ones. As frequency approaches the system's natural frequency, survival times is dramatically reduced, hinting for resonance effects, that destabilize the system and drive it faster to collapse. Last, there is a fairly low sensitivity to the disturbance occurrence time point and activity duration change.

An equivalent image is seen regarding the degradation time period, as Figure 149. Except for strategies 1,2 which maintain their stability and insensitivity to changing uncertainty, the others significantly increase the degradation time period with increasing disturbance magnitude.. The frequency dependency is more complex,

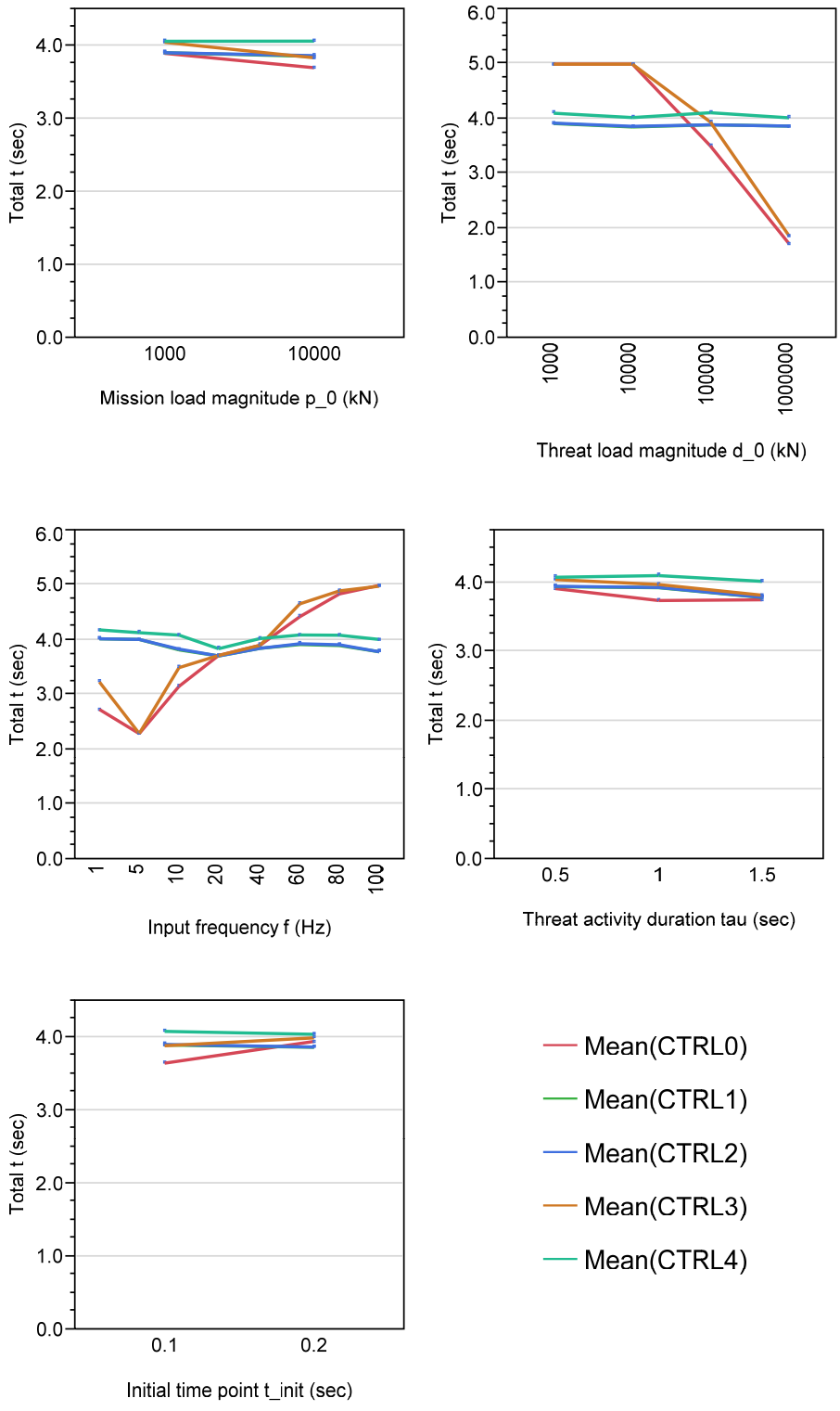


Figure 148: Variation in survival times with different control strategies

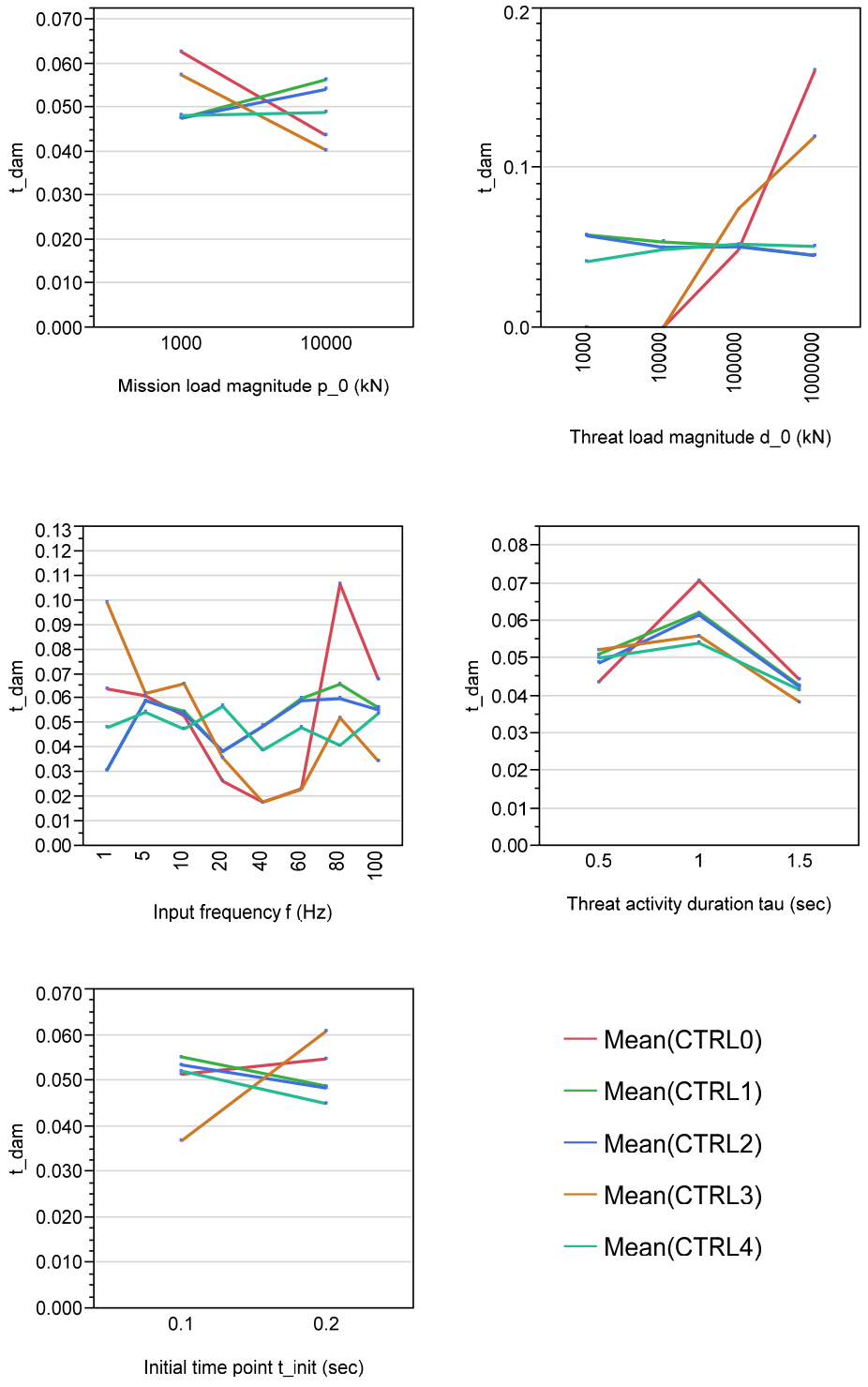


Figure 149: Degradation time period with different control strategies

otherwise hinting how much of a significant impact this uncertainty variable has for periodic inputs to dynamical systems. Disturbance occurrence and duration play a more significant role for degradation time, yet without the complexity and non-smoothness of the frequency response. Regarding the maximum damage, behavior responses are very similar to these for survival times, with same complexities and stabilities, as discussed earlier. Maximum degradation analysis is presented in Figure 150.

Continuing on the recoverability part of the system's response, Figure 151 contains the analysis for the restoration offset. The expected response for a resilient system requires a low offset. Besides, this requirement, robustness requirements indicate that the offset is not affected by uncertainty. This is the case for strategies 1, and 2, while with strategies 1, 3 and 4, the offset increases with increasing load magnitude, and input frequencies closer to the natural frequency.

It is interesting however, that recovery time is fixed for all strategies, as Figure 152 indicates. Thus recovery time, does not appear to relate to the reconfiguration strategy, rather than the main topology of the system itself.

Combining information on the recovery offset, along with the recovery time, the average recovery rate is estimated and presented in Figure 153. As with the recovery offset, the recovery rate presents an analogous response to uncertainty, since the recovery time is fixed and independent of uncertainty for all control strategies.

To perform analysis for the "absorb" function capacity, the time-averaged MC degradation is necessary to be calculated. Figure 154 presents the analysis results, which do connect with the rigor behind the stability and insensitivity to change of alternatives 1 and 2. Regarding the impact of threat magnitude however, there is a counterintuitive outcome. The response, which mainly depends on MC degradation is reducing for increasing magnitude values. Unlike earlier metrics where there was a form of degradation that would always increase with magnitude, in the present case,

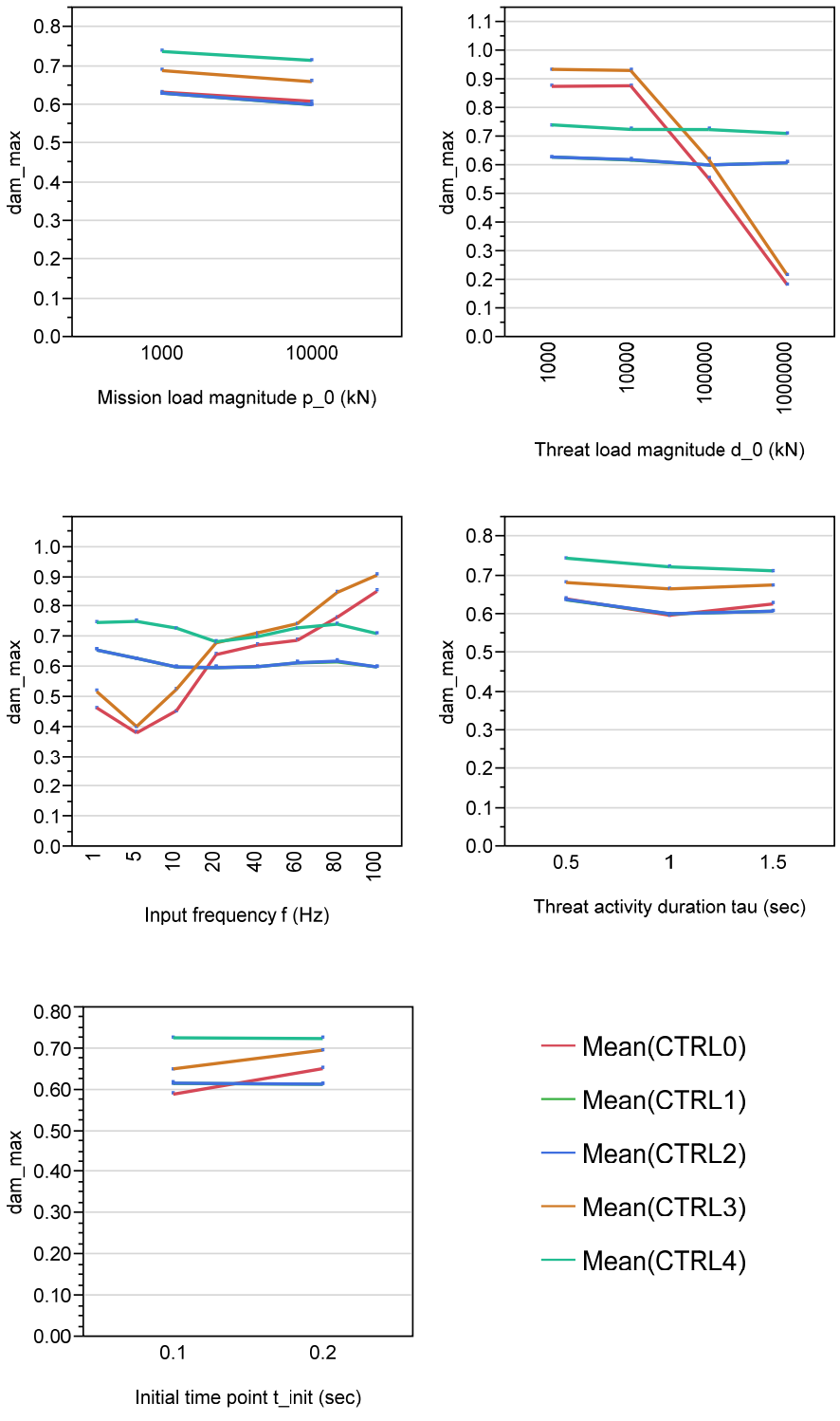


Figure 150: Maximum degradation with different control strategies

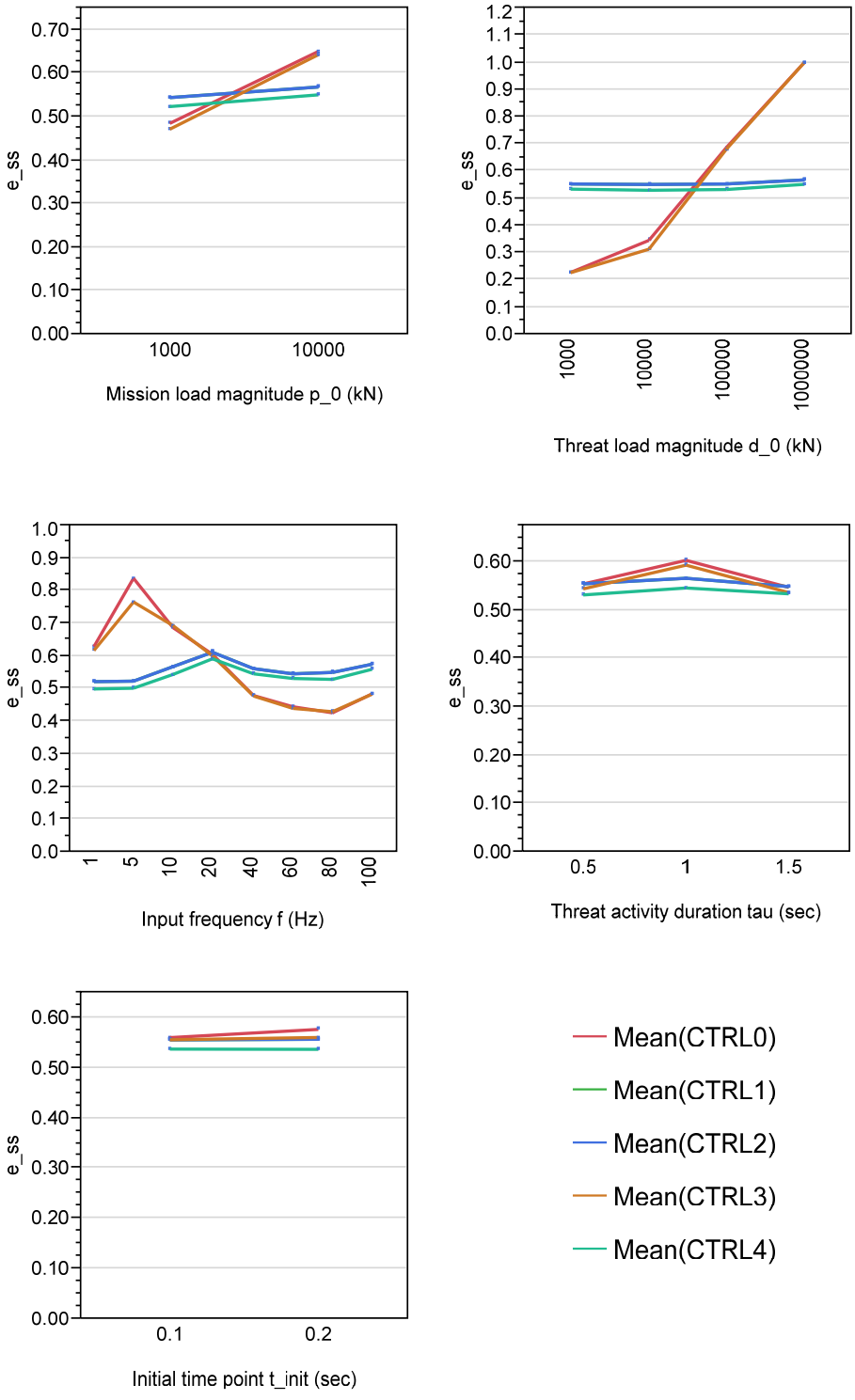


Figure 151: Recovery offset with different control strategies

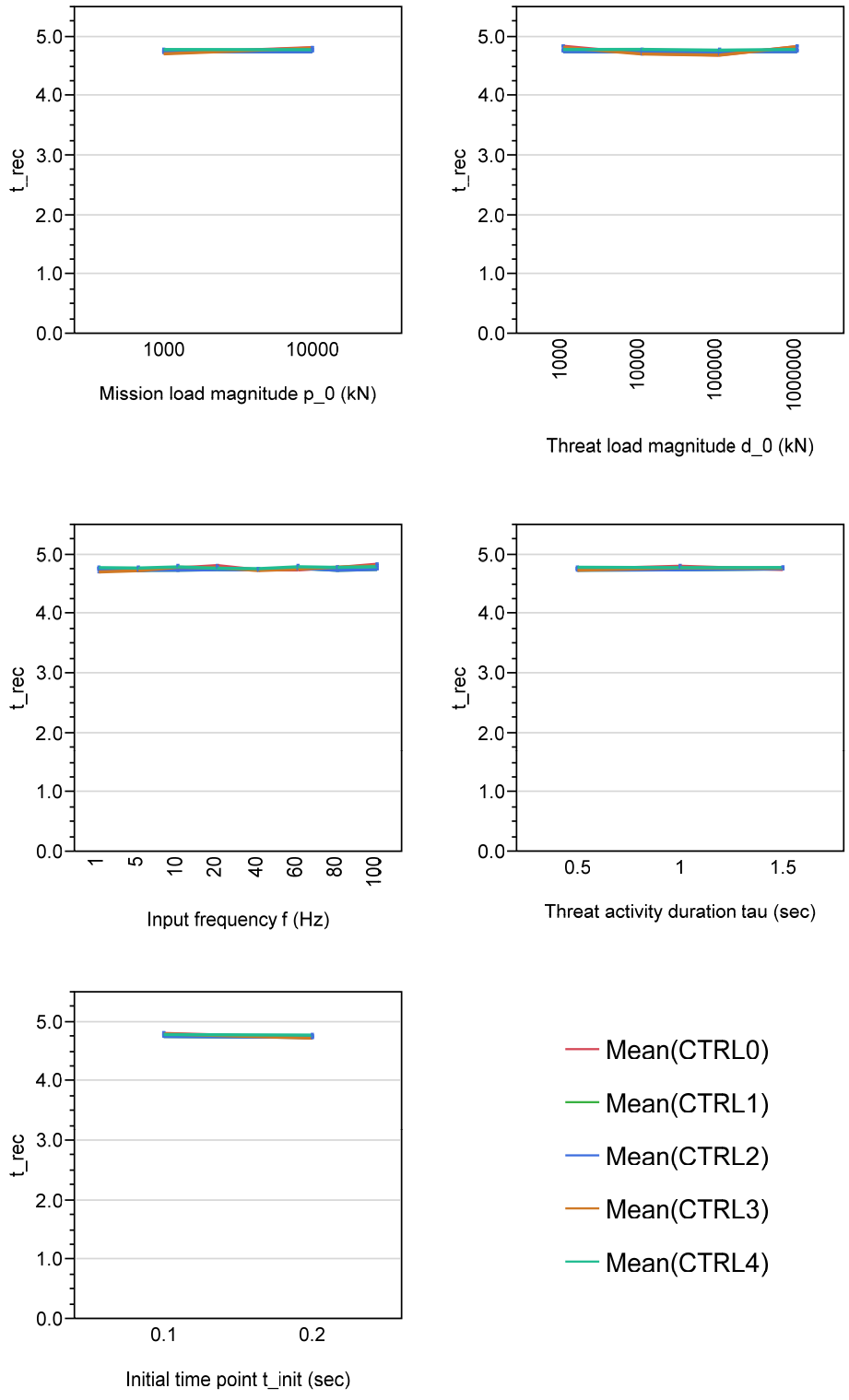


Figure 152: Recovery time with different control strategies

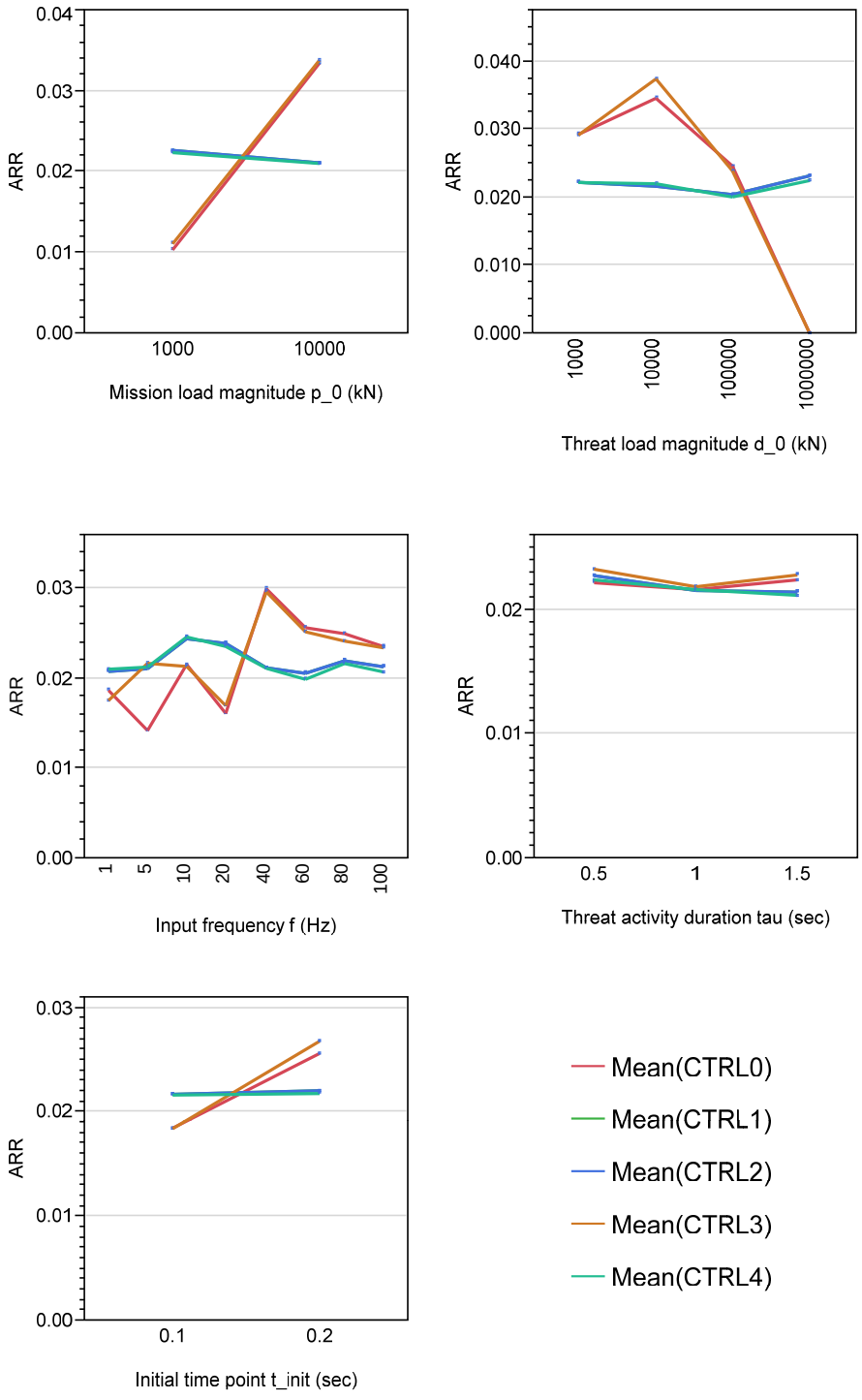


Figure 153: Recovery rate with different control strategies

the current metric is time averaged. As it was earlier observed, lower magnitude settings result in larger system life expectancies, or survival times. It is thus the effects of a larger survival time that promotes higher metric values, and are overcoming the effects of degradation, that would otherwise dominate.

The time-averaged MC degradation is the basis for estimating the degradation-to-threat effects ratio. At this point, the final assessment on the system's ability to absorb the effects of uncertainty factors can be made. Not much different from the evidence discovered earlier, the D/T response allows for the alternatives CTRL1, and CTRL2 to be distinguished as being stable and insensitive to the effects of changing magnitude, frequency and duration of the threat representing input periodic signal. Figure 155 is supporting this point, while a case is made on how the reconfiguration strategy can actually make a difference in improving the system's ability to absorb the effects of a disturbance and be robust to change.

To complete this study, the RTO response is providing an estimate on how the alternative strategies affect the ability of the system to "adapt" to change, and the results are presented in Figure 156.

5.5 Summary of findings

Chapter 5 presented all efforts on the development of the resilience assessment technique. With the use of a canonical problem that is transparent, and easy to understand, a series of metrics was developed and tested. In an effort to better understand the metrics of the framework as, well as all the critical measures for supporting system resilience assessment, options were explored on combining metrics into aggregates for high level resilience representation. The basic assessment procedure returned estimations on the three resilience functions, "adapt", "absorb" and restore,, based on MC experiments with varying uncertainty factors. Significant uncertainty factors, such as input magnitude or input frequency have been identified and distinguished as the

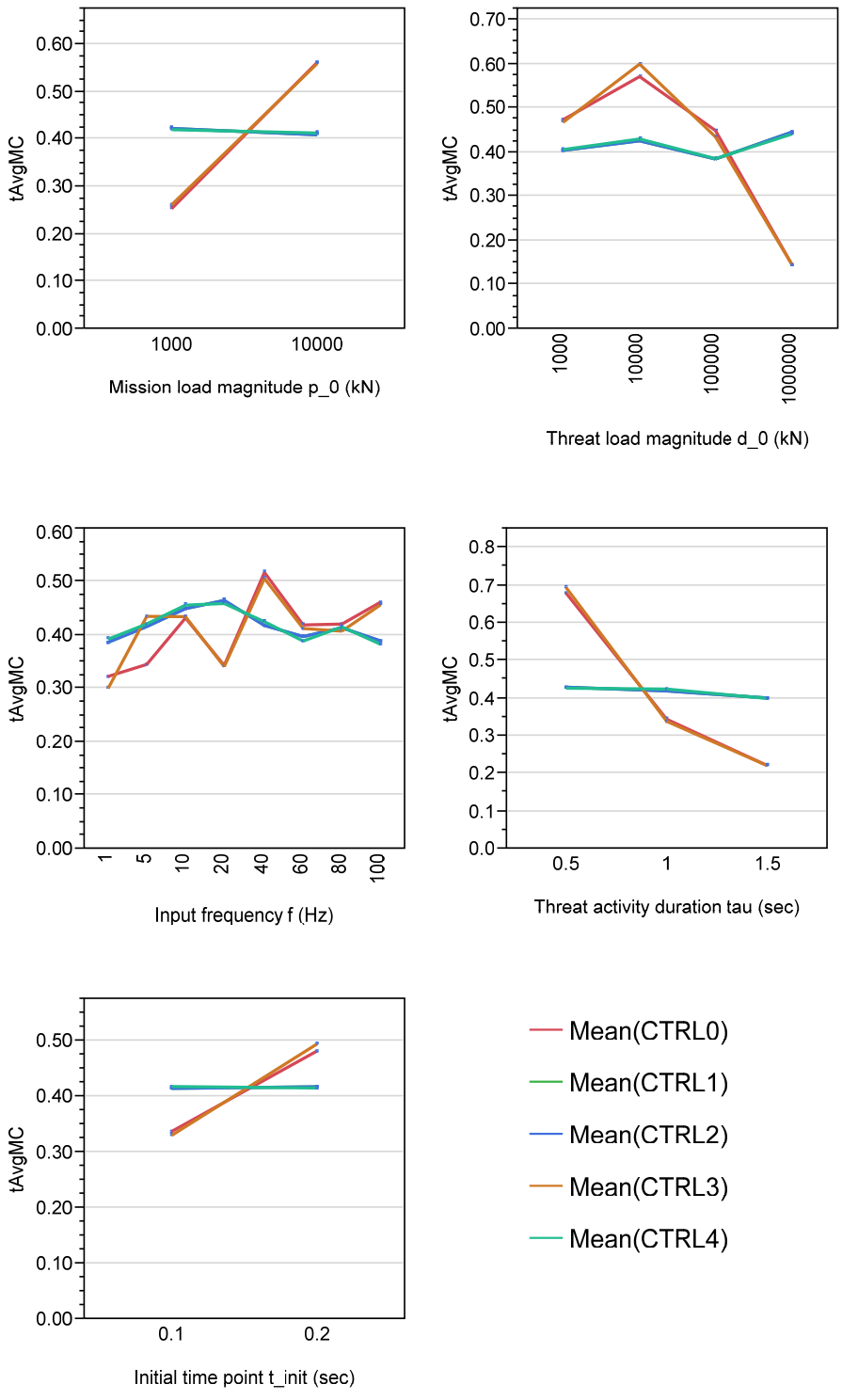


Figure 154: Time-averaged performance degradation with different control strategies

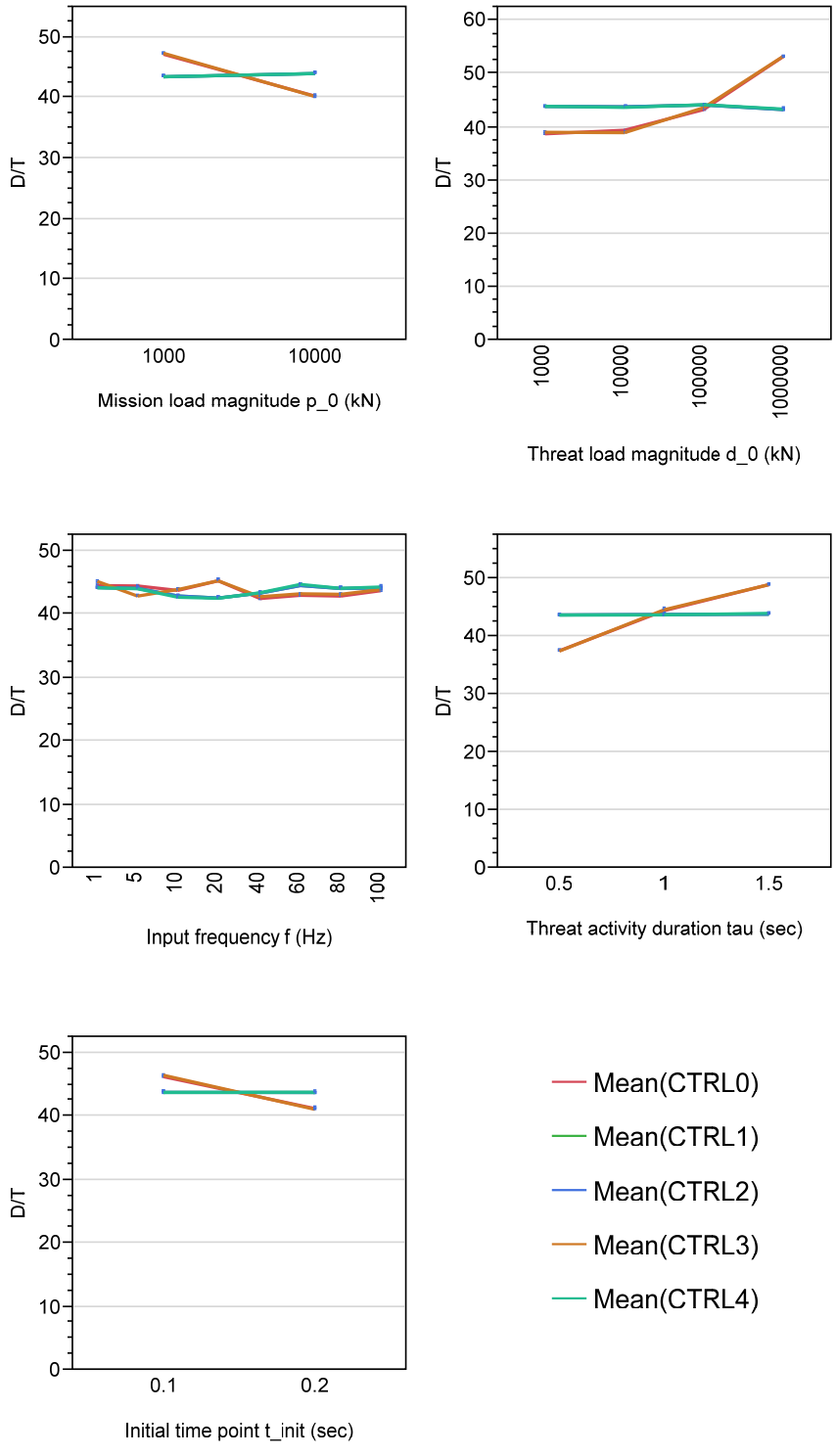


Figure 155: Degradation-to-threat ratio with different control strategies

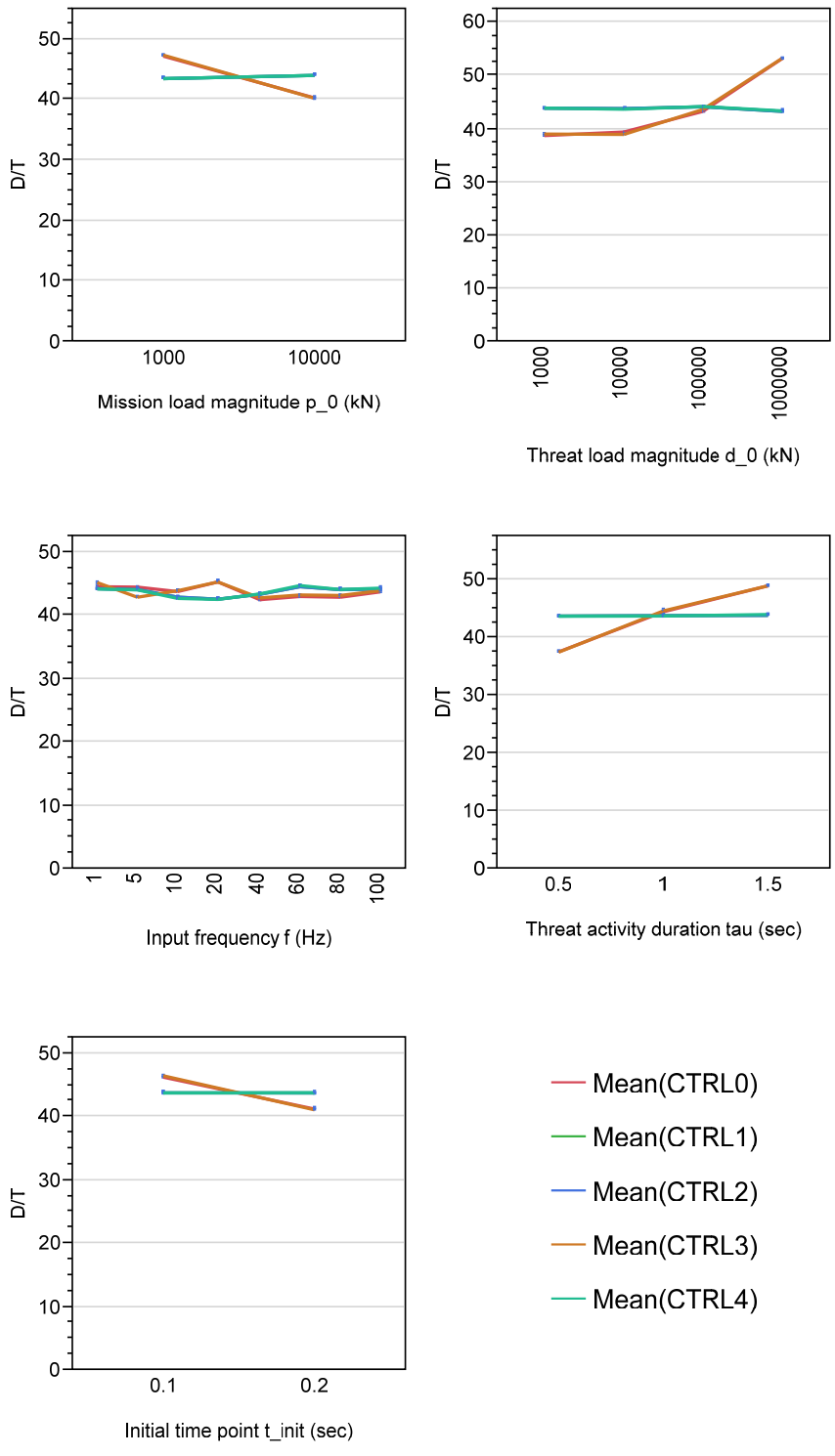


Figure 156: Relative total threshold offset RTO with different control strategies

most influencing uncertainty factors on the resilience of dynamical systems. Comparative assessments, allowed for the investigation of the impact of alternative control strategies, or the ability of the system to naturally absorb the effects of change. In conclusion, the technique has successfully demonstrated its ability to investigate resilience against uncertainty, to allow for evaluation and comparison of enhancement solutions for improving resilience and survivability, as well as to support a resilience-based design space exploration.

CHAPTER VI

RESILIENCE ASSESSMENT OF A NAVAL COOLING NETWORK ARCHITECTURE

With Chapter 4 and Chapter 5 discussing the formulation and the development of the resilience assessment technique, respectively, the present chapter's objective is to demonstrate the applicability of the resilience assessment technique on a larger scale architecture, as well as to discuss findings on the investigation of topological modifications for resilience and improved system survivability. The experiments concentrate on resilience assessment of system baseline, as well as the effects of redundancy and controller effects on the three resilience capacities.

6.1 Overview of method demonstration

The general procedure for the resilience assessment is identical to the process that was followed in Chapter 5 for the canonical SMD system problem. While the basic idea is the same, however there have been adjustments on mapping of system variables to resilience capacities and definitions for system health and mission capability. The basic steps that were taken for the method demonstration are:

1. Define and characterize system baseline.
2. Setup the modeling & simulation environment.
3. Generate the simulation scenarios.
4. Resilience assessment for the system baseline
5. Effects of topology and control system

6.1.1 Baseline configuration overview

The selection of a system baseline for the cooling network is driven by the mission requirements, as well as the configuration of interacting subsystems. The piping architecture, the number of essential components, such as valves, pumps, and heat exchangers, as well as their placement, depend on the number, the connectivity and the location of the onboard ship systems. Their sizing depends on mission requirements, as well as safety directives. The objective is ensure that good system health is maintained, and the system does not experience degradations that could lead to catastrophic failures. At the same time, the cooling network must be maintain its mission capability along with its good health, and continuously support both the vital and non-vital loads.

For the particular example, the system baseline is a smaller scale version of a naval combatant's chilled water system network. Except for the vital components, this topology includes 10 flow meters that have been placed in various locations, in order to monitor water flow rates. To control flow rates on different network locations, a total of 32 valves have been placed in key locations. The valves are controlled by a simple, rule-based, ideal response controller (developed by Icosystem Corp.), and it is part of the current model implementation. Figure 157 gives an overview of the network baseline topology.

6.1.2 Modeling & simulation facility

The system testing configuration is an integrated Java application that consists of the dynamic system model and the rule-based ideal response controller. This integrated simulation facility is the dynamical modeling & simulation environment that will be used for performing the main demonstration experiments. The module of the facility which integrates the power system with the cooling network is a monolithic

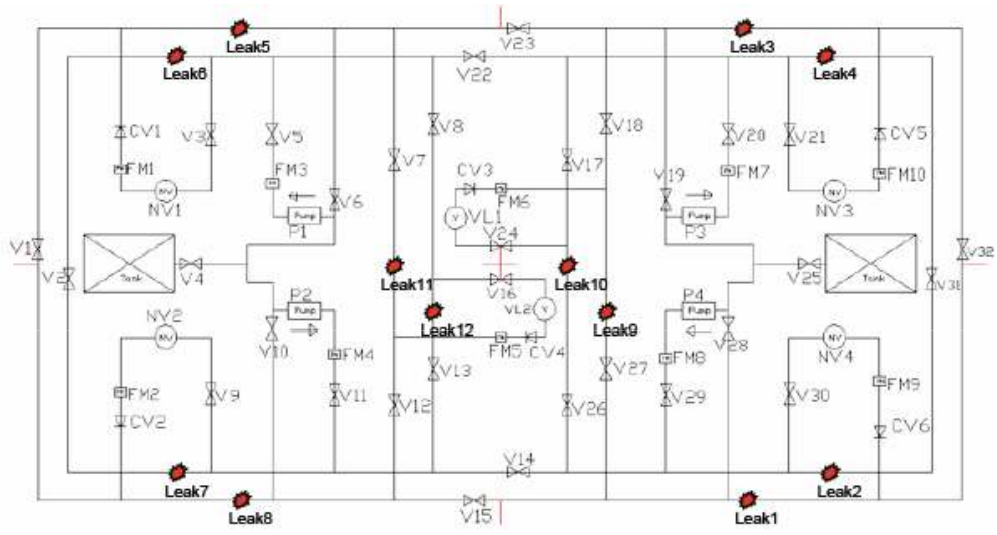


Figure 157: Baseline configuration for the cooling network

MATLAB/Simulink implementation [179]. To improve simulation speed, this monolithic module is not represented in the top level facility by its original, but through compiled executables. It also receives the input scenario information, which contains the prescribed damage input to the system.

Except for allowing faults as status inputs, this particular facility has been augmented to include leaks on different system locations, as well as to model the effects of a leak and allow the user to observe the impact on the simulation development. Thus, a list of leak locations plays the role of the damage input to the system. The monolithic executable runs a case for a given scenario, and at the end of each time step, it passes the output information to the Java implemented rule-based ideal response controller. As implied by its name, the controller selects the ideal combination of valves that must be shut, in order to ensure that the part of the network that is experiencing the leak, is isolated from the rest of the system. As the controller takes action on setting the valve commands, the monolithic executable receives back this information and propagates it to the valve actuators. The appropriate valves are shut and the system dynamically adjust itself to the new reconfigured state of operation. This integrated scheme for the modeling and simulation environment is depicted in

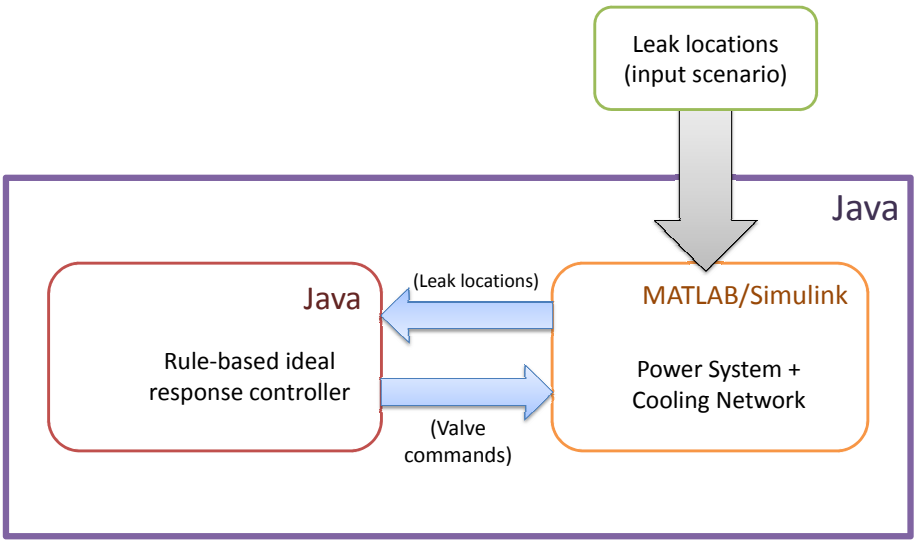


Figure 158: Modeling and simulation environment structure

Figure 158, while a view of the chilled water network implementation in the Java environment is shown in Figure 159.

6.2 Experimental setup

The next step of the assessment technique, commands for setting up the necessary experiments that need to be run for the analysis. This includes the formulation of scenarios for modeling operational uncertainty, and for the particular study, the factors are the leak locations, as well as the number of leaks that are preselected to occur for each simulation run. Each simulation run is scheduled for a 2 sec period. With a total of 12 leak locations, the scenario generator returns $2^{12} = 4096$ different leak combinations. The actual time for a 2.2-sec simulation time period is about 30 seconds, thus it would be reasonably affordable to execute all 4096 different cases for each study.

In order to generate the case input settings, a full factorial DOE has been constructed, with each DOE case representing a complete dynamic scenario, along the lines of DOE tables that have been used for the canonical problem. The scenario

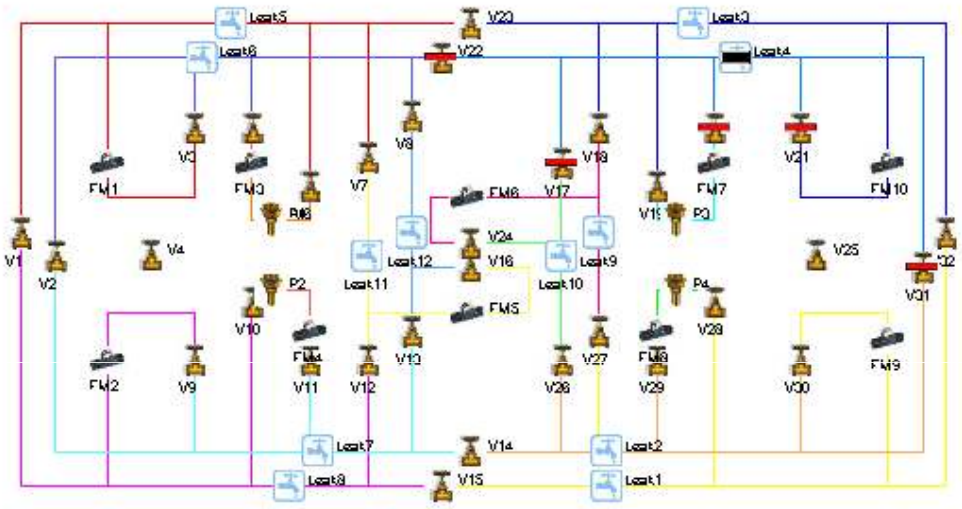


Figure 159: Baseline cooling network model

format involves a 12-element array with a "1" denoting an active leak, and a "0" implying no leaks, for each index that represents the corresponding leak location. The pre-determined possible leak locations are also listed in Figures 157 and 159. The latter is a visualization of the network that serves as a GUI, where the user can see what are the specified leak locations, and which valves are being shut down, as part of the controller's response.

In terms of the system's performance during a simulation, this is obtained through the flow meter readings. The mass flow rates for the coolant are available in certain locations, where the 10 flow meters are placed. A typical simulation response is shown in Figure 160, with all flow rate time histories for all meter locations. The rates are measured in gal/min and the time step for the simulation is 0.1 sec.

Last, two studies have been planned for supporting Hypotheses 2 and 3, with experiments on the cooling network model. Experiments 1.1 to 1.3 refer to the system baseline, as it is described by Figure 159. With the 32-valve configuration, survival time measurements and resilience capacity estimations take place, and these are analyzed against the leak combinations that represent operational system uncertainty. Experiments 1.4 and 1.5 are planned for investigating the effects on the total number

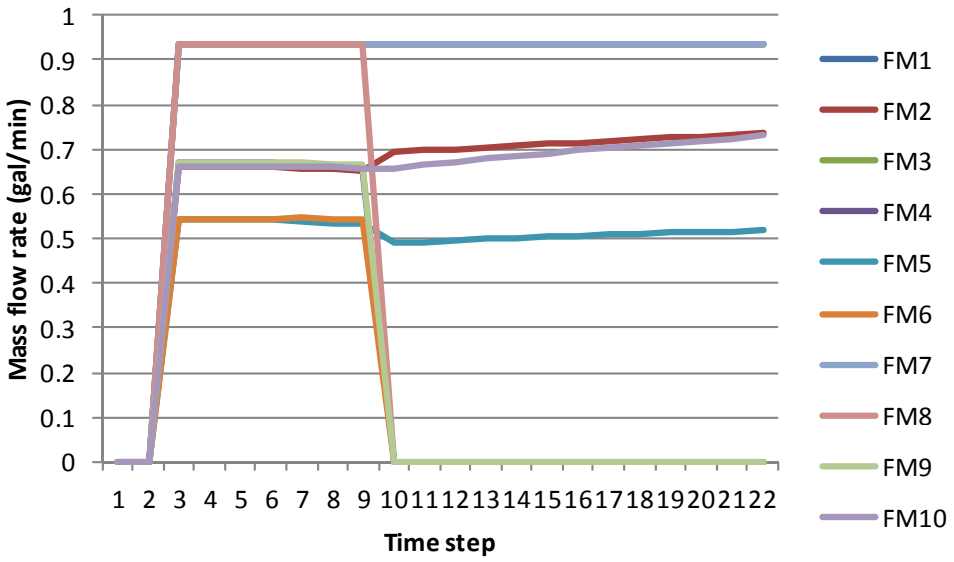
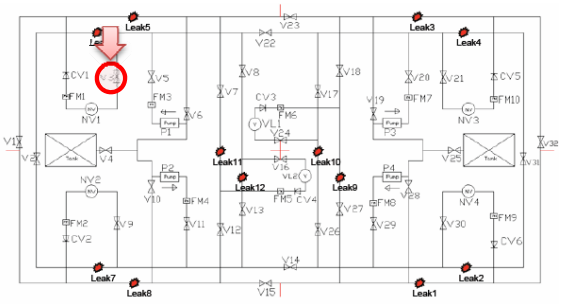


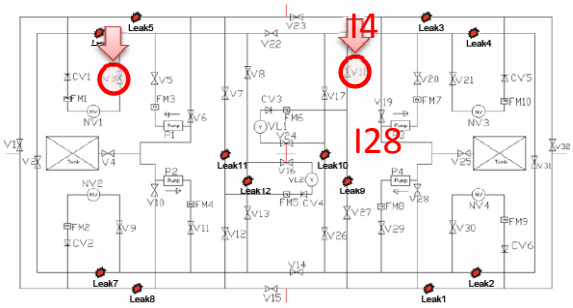
Figure 160: Typical flow response curves for system baseline

of valves and the controller on the resilience metrics, in a study similar to that of the canonical problem.

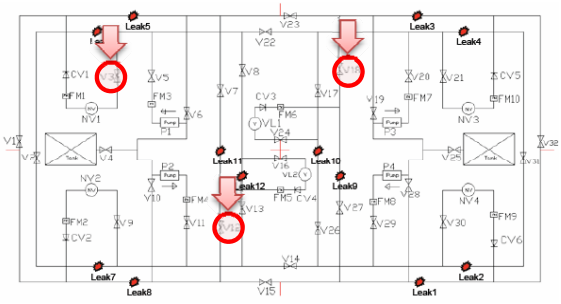
For Experiment 1.4, it is the aspect of architecture robustness that is being tested against the resilience capacities. For this purpose, six modified topologies have been defined and implemented within the simulation environment. The total number of valves is varying across the alternative configurations, ranging from 26 to 32 valves. The purpose is to observe the robustness of both the topology and the controller with a decreasing number of available valves. In other words, the effects on the resilience capacities is solicited, as reconfigurability is degraded through reducing the number of valves. Figure 161 outlines the different topologies that have been tested. For Experiment 1.5, the sole impact of the controller is the outcome of interest, while demonstrating the need for reconfigurability and control, for enabling system adaptability.



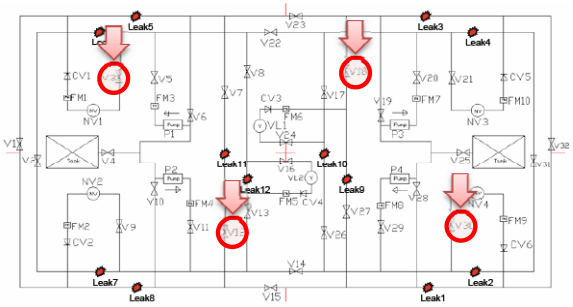
31-Valve Configuration



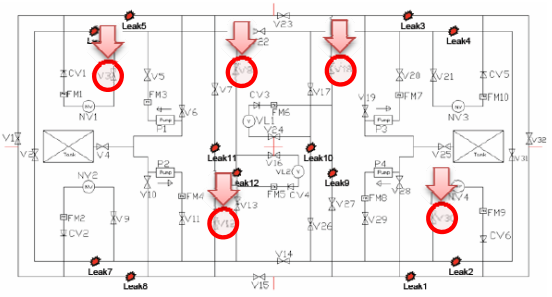
30-Valve Configuration



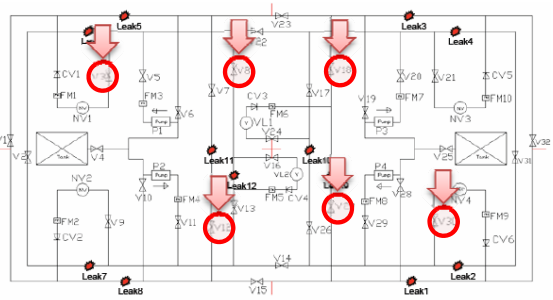
29-Valve Configuration



28-Valve Configuration



27-Valve Configuration



26-Valve Configuration

Figure 161: Alternative topologies for robustness testing and resilience effects investigation

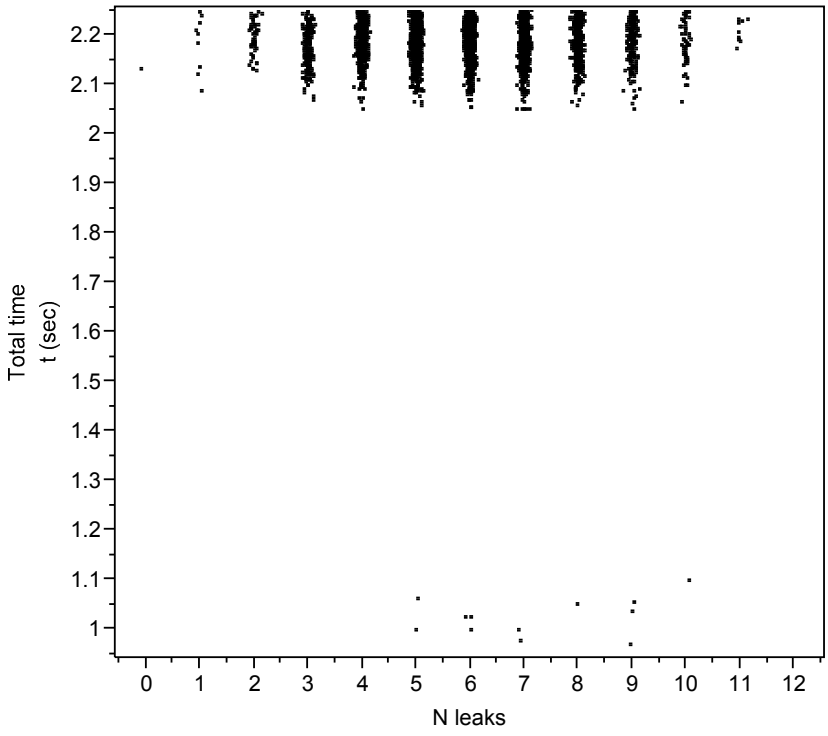


Figure 162: System activity duration with varying number of leaks

6.3 Resilience analysis for network baseline

In this section, the resilience assessment technique is demonstrated for the 32-valve configuration, with respect to the full factorial of 4096 scenario cases. The results cover Experiments 1.1 to 1.3.

6.3.1 Experiment 1.1 - Recoverability and survivability under uncertainty

Experiment 1.1 is focusing on system recovery and survivability, for the 4096 cases on all the combinations of leaks. With the use of the ideal response controller, the system demonstrated a survival rate close to 1, namely almost in all cases, the controller has been very robust. As the life time distribution shows in Figure 162, there are only a few cases where the system collapses before the end of the simulation, mostly around the $t = 1$ sec mark.

Damage propagation in this context, refers to capability degradation. For the

particular system, capability degradation in a flow meter FM_i is defined as the difference of $MC(t)$ for the particular configuration and leak combination, minus the $MC_{ideal}(t)$ for the same configuration and without any leaks on the scenario. Thus total mission capability is defined as:

$$MC = 1/(1 + \sum_{i=1}^{10} \Delta\dot{m}_i^{FM}) \tag{76}$$

where $DeltaMC_i^{FM}$ is the difference of a flow meter's $\dot{m}_i^{FM}$ reading minus to the corresponding ideal reading $\dot{m}_i^{FMideal}$, namely

$$\Delta\dot{m}_i^{FM} = \left|\dot{m}_i^{FM} - \dot{m}_i^{FMideal}\right| \tag{77}$$

Most damage propagation calculations, as well as estimations on the resilience capacities are based on MC data. The MC value for the ideal case is 1, thus degradation is defined as:

$$MC_{deg} = 1 - MC \tag{78}$$

Since MC varies from 0 to 1, with 1 as the best capability (often by-design capability), degradation of capability will adapt to the same range, with 1 denoting maximum degradation, where the system is not capable to perform its mission.

Maximum damage is the maximum degradation point for a given time history of $MC(t)$. Figure 163 contains the frequency plot for the maximum damage points. The shape of the distribution appears to closely follow a normal distribution, with a mean of 0.5, and a standard deviation of 0.144. Based on the frequency plot, the same figure also contains the CDF distribution.

Similarly, Figure 164 lists the distribution for the damage propagation rate DPR. The DPR is the average propagation rate of the degradation front. It is the ratio of the total degradation over the time it took for that degradation to occur. The mean is 2.5 (MC degradation per sec) and the standard deviation is 0.721.

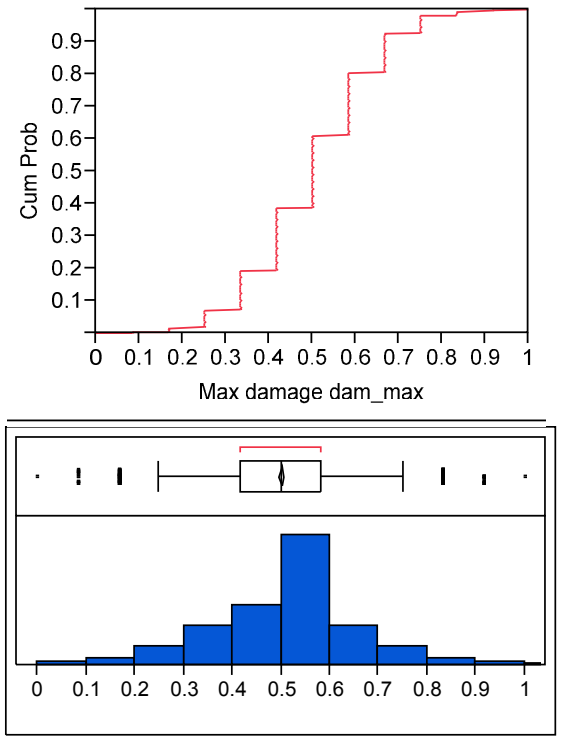


Figure 163: Maximum damage point distribution

6.3.2 Experiment 1.2 - Resilience capacities under uncertainty

In Experiment 1.2, the capacities for the three resilience functions are brought into focus. Changing trends for the capacity measures were documented against increasing number of total leaks. In the baseline configuration, the restore function is described by four metrics, namely the maximum degradation, the recovery time period, the restoration offset and the average recovery rate. Table 5 lists the average values for all four metrics along with their standard deviations.

Table 5: Restore function capacity baseline values

	Mean	Std deviation
Max degradation (MC=[0,1])	0.339	0.109
Recovery time period (sec)	0.475	0.352
Restoration Offset (MC=[0,1])	0.328	0.08
Average recovery rate (MC/sec)	0.0009	0.076

To put observations into perspective, the maximum degradation throughout the

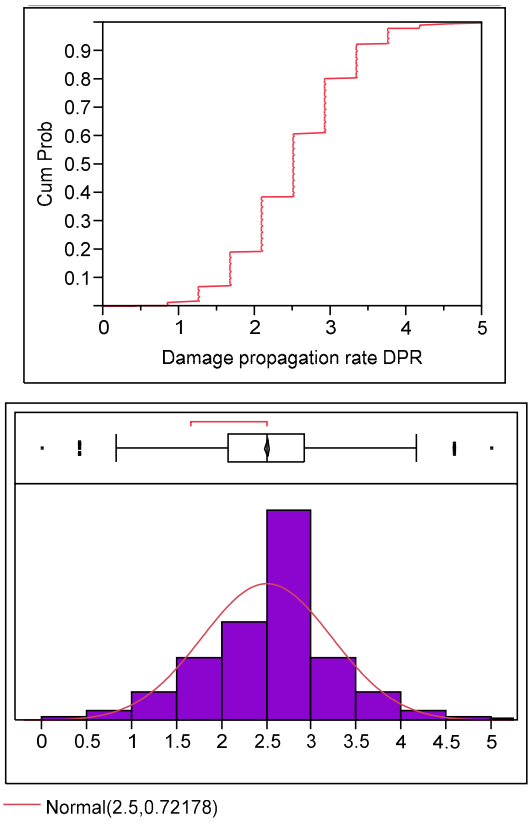


Figure 164: Damage propagation rate DPR distribution

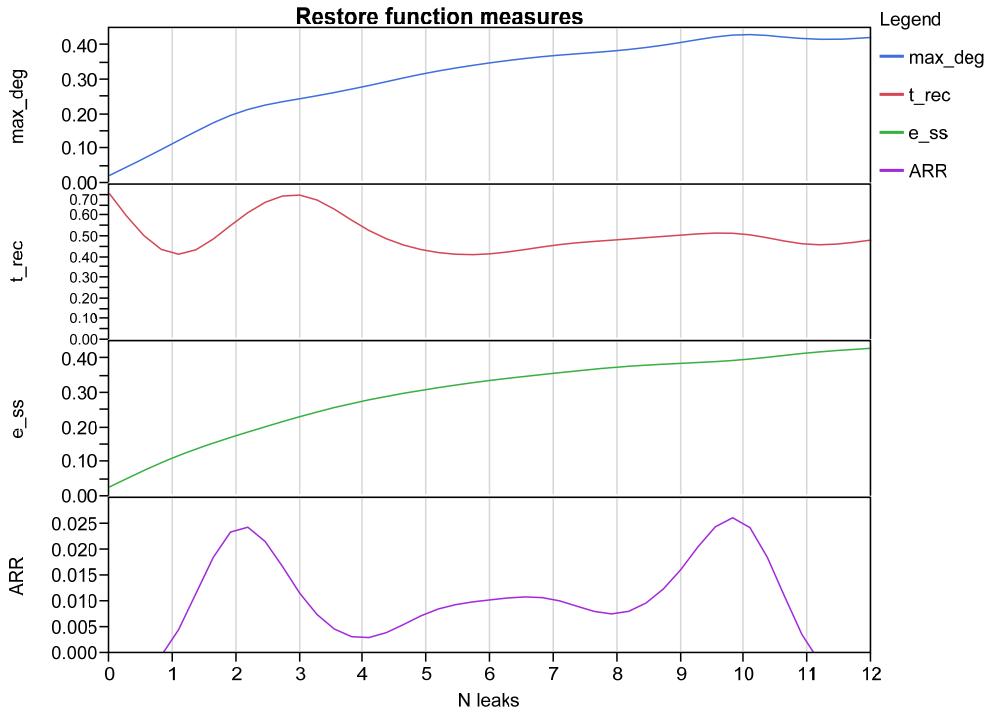


Figure 165: Restore capacity estimates with leaks

entire range of uncertainty effects, are limited to a third of the total system's capability. The recovery time is about a quarter of a nominal simulation run, while the average offset is also a third of the MC capability. The latter is explained by the low recovery rate, which implies that either the restoration falls short of the original MC values, or that recovery needs to occur much faster than the nominal simulation time, thus a larger gradient fails to build up.

Figure 165 presents the variation of the four restore function capacity estimates with the increasing number leaks that the system is experiencing. The maximum degradation is increasing with the increasing leaks and that makes perfect sense, as this is causing greater deviation of the mass flow rate in each meter, from the ideal response value, which has been used as a reference. The degradation peaks at 10 leaks, and reaches a plateau. The recovery times also vary with the increasing leaks, though without a monotonous trend, but with local peaks. Thus, recovery time is

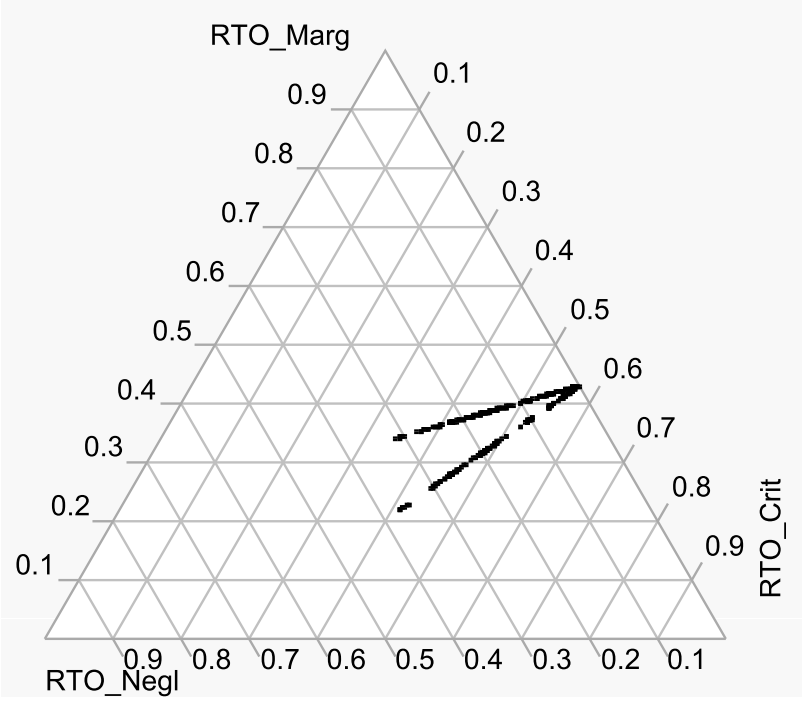


Figure 166: Ternary plot for three partial RTO offsets

varying with the number of leaks, yet the increasing leaks, is not the sole factor of recovery time variation, as other interactions are hinted. The restoration offset follows a similar trend to the maximum degradation, and relates higher offsets to increasing number of leaks. The average recovery rate varies with the number of leaks, yet not with a unique trend. Local extreme points are observed, but the overall behavior does not strongly depend on the number of leaks, as it probably does with the particular recovery mechanism that takes place. In conclusion, passive observed responses, such as the degradation and the restoration offset do depend on uncertainty effects, through increasing number of leaks. Restoration, which is seen as an active response on the system's behalf, while affected by leak related uncertainty, is mostly determined by the interaction of other factors, such as the controller and system reconfigurability.

The adapt function, is described by the total relative threshold offset RTO, along

with the partial, offsets that refer to each one of the three reference thresholds. Similarly to the restore function, the adapt function for the baseline analysis is characterized by the average values for the offsets, and the results of the assessment are shown in Table 6. Another way to view the partial RTO estimates is through the ternary plot of FIgure 166.

Table 6: Adapt function capacity baseline values

	Mean	Std deviation
Total RTO	0.489	0.0829
RTO-Negligible threshold (MC=0.8)	0.185	0.134
RTO-Marginal threshold (MC=0.6)	0.463	0.113
RTO-Critical threshold (MC=0.4)	0.628	0.082

Starting from the partial thresholds, average values carry different implications for the different thresholds. That is, a small offset from the negligible threshold is often acceptable or even desirable, but it is exactly the opposite for the critical threshold, where the system must remain away to ensure that a catastrophic failure will not occur. This logic is indeed depicted through the average values in Table 6, where the offset from the negligible threshold is about 0.2, while the critical threshold offset is 0.628. Figure 167 presents the impact of leak related uncertainty to the RTO offset. As expected, the increasing number of leaks induce further MC degradation, which translates to responses that are reaching closer to the critical thresholds, and thus reducing the partial RTO estimates.

The absorb function, that is linked to system robustness is characterized by the time-averaged MC degradation, and furthermore by the degradation-to-threat input ration D/T. Table 7 contains the average values for both metrics. The former is an estimate of robustness, while the latter expends this definition, by bringing in the perspective of the intensity of the input, that the system must respond to. A resilient system must maintain low degradations over time, thus a low time-averaged MC degradation, and D/T response is desired. Regarding the effects of increasing

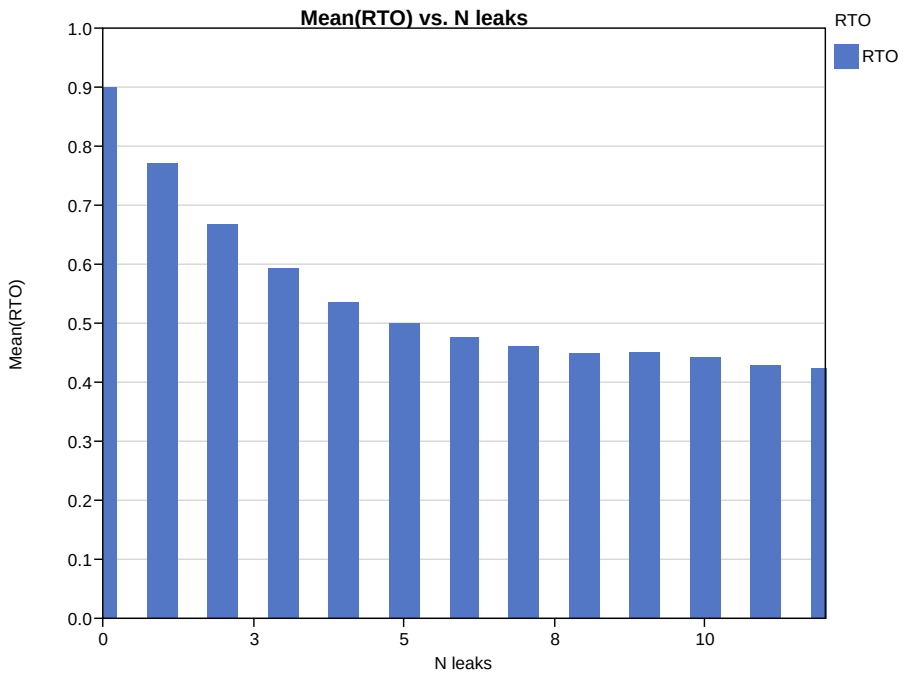


Figure 167: Adapt capacity estimates with leaks

number of leaks, the D/T average is dropping as the system is experiencing more leaks, as observed by Figure 168. While degradation is increasing, the drop is the result of the increasing threat level, in the form of increasing uncertainty. A lower D/T however is desired, and if the effects of the increasing leak number is overshadowing an increasing (but, at a low rate) degradation, then, this response implies a plateau in degradation after a certain number of leaks. The previous assessment, is also in accordance to the top response of Figure 165.

Table 7: Absorb function capacity baseline values

	Mean	Std deviation
t-Avg MC degradation	1.95	1.13
Degradation-to-threat D/T	0.721	0.931

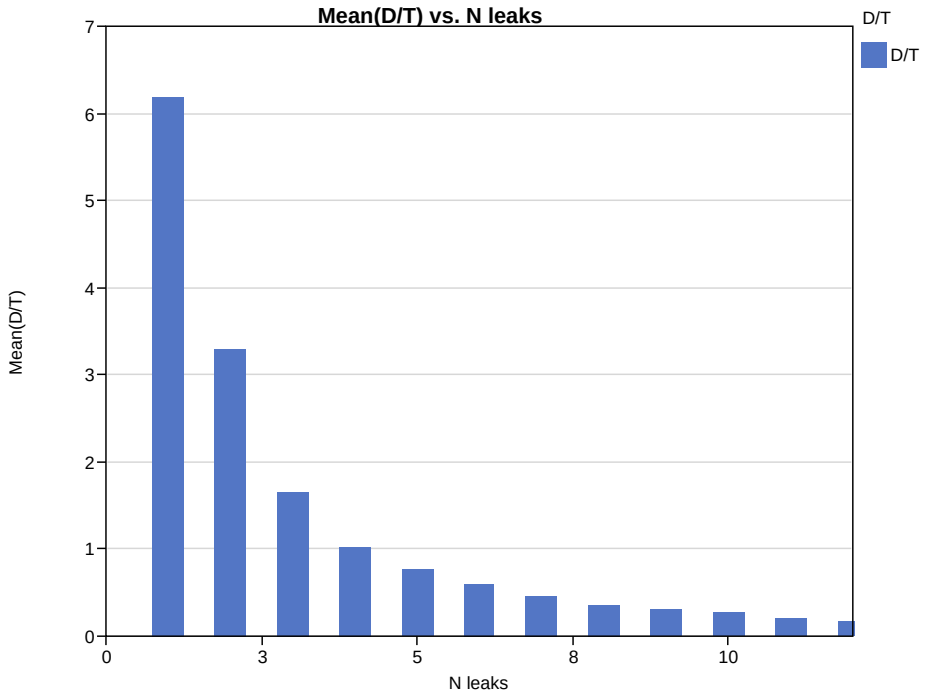


Figure 168: Absorb capacity estimates with leaks

6.3.3 Experiment 1.3 - Correlation of capacities under uncertainty

In the context of Experiment 1.3, the correlations between the resilience capacity measures are investigated. The system's ability to restore its health and mission operations, is derived by the $MC(t)$ time histories. However, the other two capacities of adapt and absorb functions are inferred by restoration and recovery observations, in accordance to their respective definitions. One purpose of investigating the correlations of the observed restoration, to the metrics for adapt and absorb functions, is to confirm the validity of the definitions. Furthermore, response diagrams could also be used for design space exploration, or requirements interpretation, when it comes to associating pairs of the resilience function capacities.

Figure 169 describes the association of RTO and D/T to the maximum MC degradation, in the form of a contour plot. Most scenarios cause a maximum degradation MC_{max} of about 0.4, with lower values of RTO. Except for the requirement of higher offsets from the critical threshold, the RTO must be kept low for more adaptive

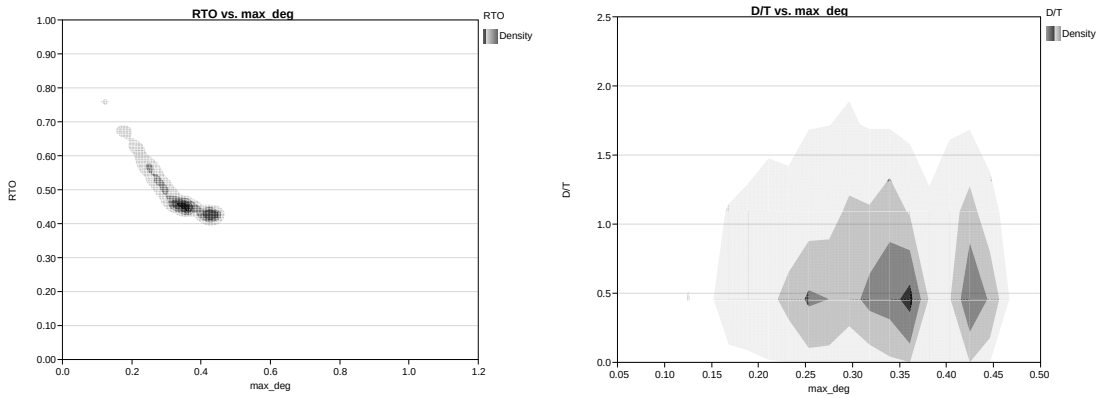


Figure 169: Capacities for adapt and absorb with max degradation

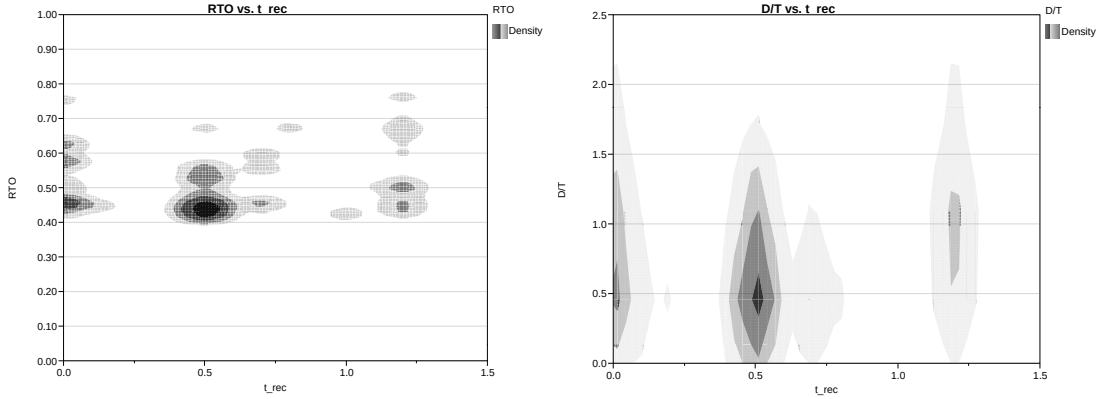


Figure 170: Capacities for adapt and absorb with recovery time

and thus more resilient systems. Similarly, the D/T ratio relates the time-averaged degradation to the input threat, and thus lower D/T values would indicate a more resilient system. Two poles are forming, as observed in 169, which indicate that the same range of D/T is linked to two different MC degradation concentrations.

The same analysis was performed with the system's recovery time values. Figure 170 shows strong concentration around 0.5 sec, whereas, there are less populated areas for 0.1 sec and 1.25 sec recoveries for fewer cases. There is no clear trend with RTO, which is a logical conclusion, given that RTO depends on threshold offsets and not in any characteristic restoration time. A similar case can be made for the recovery time against D/T, where its only contribution would be on defining the time period,

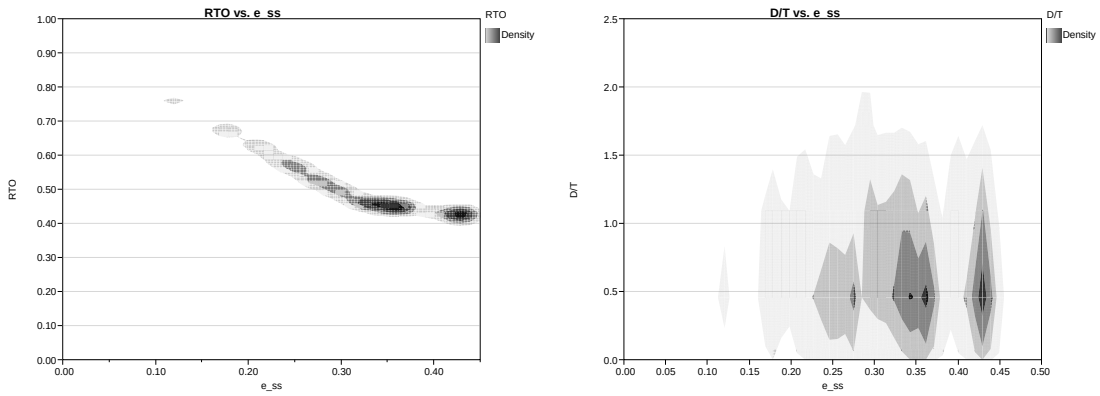


Figure 171: Capacities for adapt and absorb with restoration offset

over which the time-averaged degradation is calculated.

Figure 171 indicates that is stronger correlation of the resilience capacities to the restoration offset. There is a slight linear correlation to the RTO, which is explained from the fact that the end state of the system, as well as the path that brought it these, is also determining the offsets from the three major thresholds. As the RTO reduces, the implication is that in a collective sense, the system is closer to its major thresholds. If these lower values are due to the system reaching closer to the critical threshold, then this is also manifested by the large offsets from its original state.

Last, the response diagram between RTO and D/T is possibly of the highest interest, especially from a design space exploration perspective. As both of these metrics are the characteristic ones for the system's "adapt" and "absorb" capacities, Figure 172 is useful as a definition for a resilience-based design space. Contour concentrations would represent a given configuration. while the size of the data concentration is an estimate of the effects of uncertainty for the particular configuration. Not only used as a design space exploration enabler, this response diagram could also serve as a means of feasibility and viability analysis, when constraints have been imposed on adaptability and robustness.

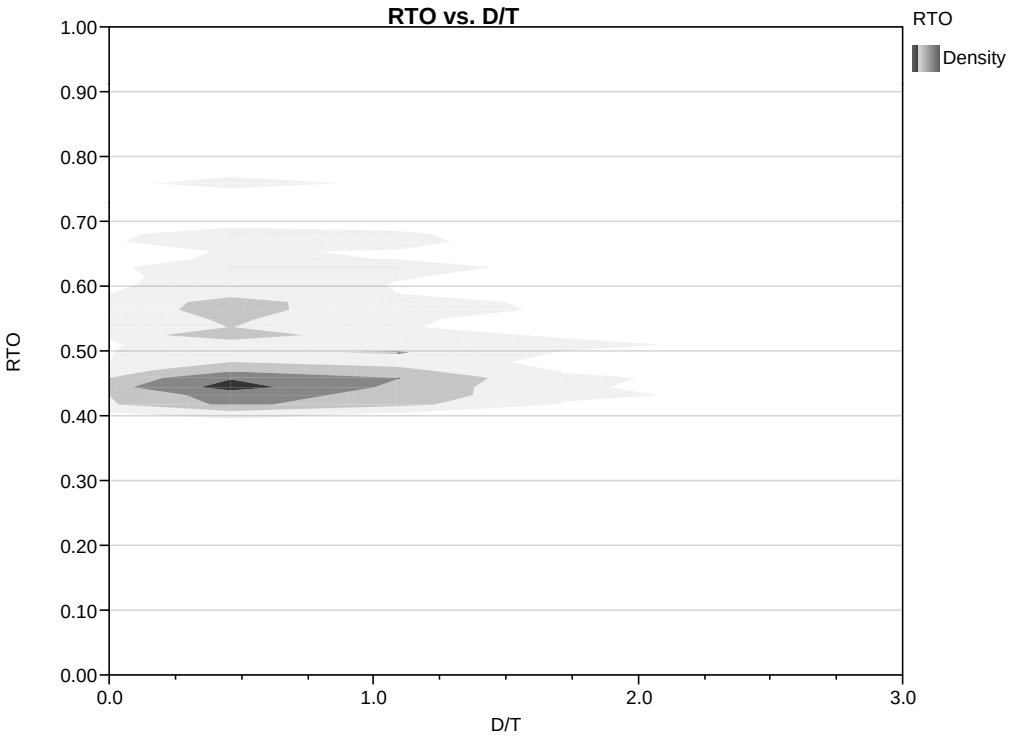


Figure 172: Capacities for adapt and absorb functions

6.4 Tradeoff studies on architecture modifications

The last part of the study for the cooling network, involves the effects on the resilience capacity estimates, with architecture modifications. Experiments 1.4 and 1.5 include plans for topology modifications, and the impact investigation of the rule-based controller. The topology modifications refer to the varying number of valves which are placed on the network, thus 6 different topologies have been formulated and tested with the resilience assessment technique.

6.4.1 Topology effects on resilience

Besides the baseline configuration of the chill water cooling network, six modified configurations have been generated. The resilience assessment technique that is proposed through this work, was applied for all modified topologies, and a comparison study has been conducted, for evaluating the impact of the modifications on recoverability,

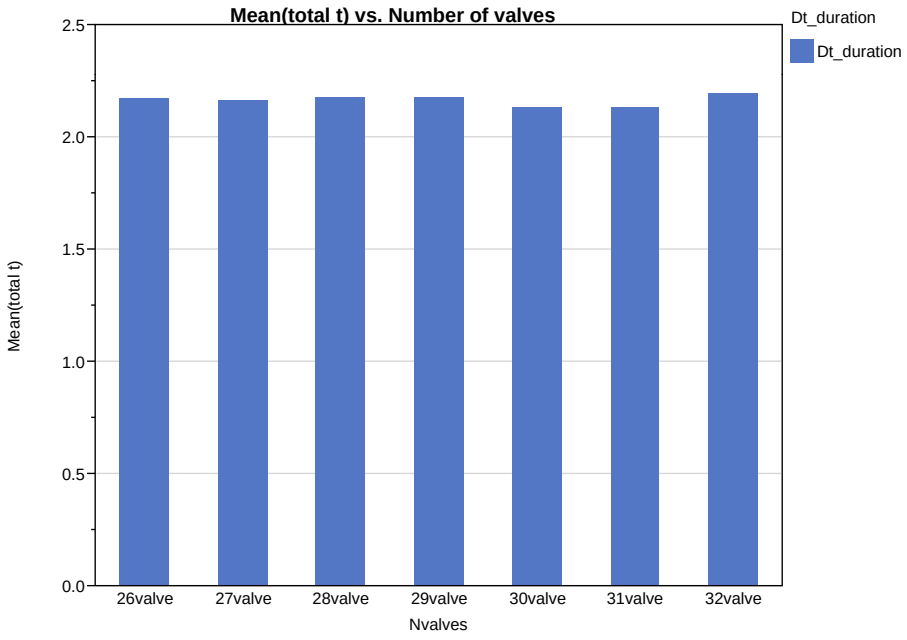


Figure 173: Survival times for seven network configurations

survivability and resilience. The topologies have been derived from the baseline (of 32 control valves total), thus returning configurations of 31, 30, 29, 28, 27, 26 control valves total for each topology.

The first step of the assessment commands for estimates on survival time, or for how long the system is in operation, until the end of the mission, or until collapse, if it becomes bound for that. Figure 173 contains a comparative bar chart that shows the averages of survival times for all seven configurations. Despite the fact that differences are marginal, it is the 32-valve configuration that has better survival times on an average basis, with the 28, and 29-valve variations to be exceptionally close. A drop in time is observed for the 30 and 31-valve configurations.

It must be understood that the baseline has been developed according to the mission requirements, and the number of valves has been decided for this particular configuration setting. Moreover, the controller has also been designed with the baseline cooling network topology, thus a degraded topology in terms of valves was not expected to return better results. However, it was surprising that the 29-valve

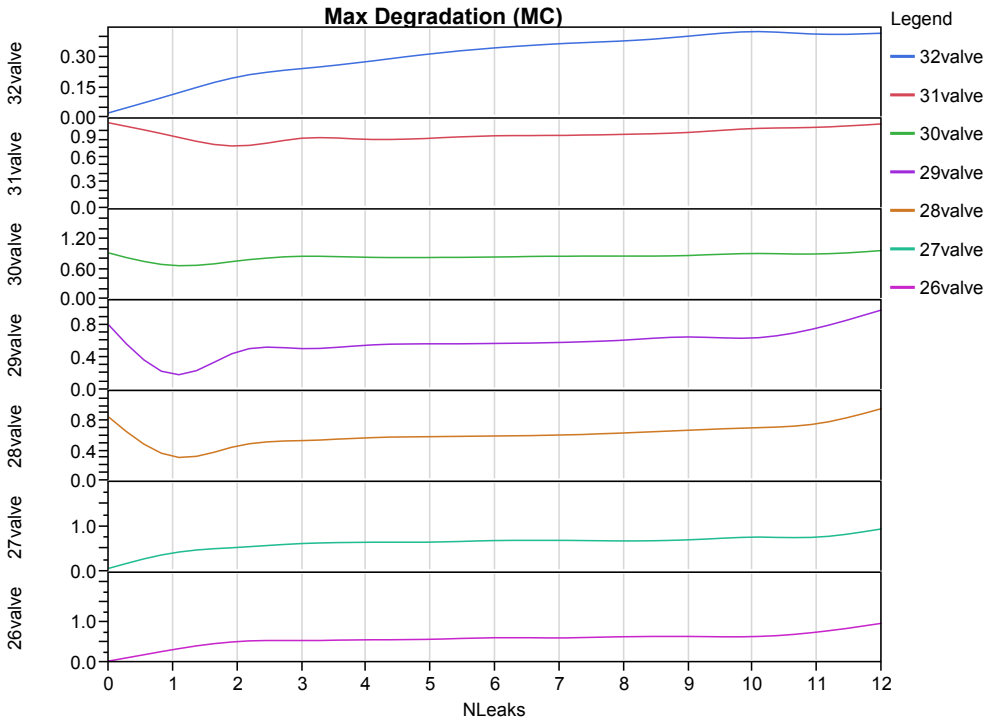


Figure 174: Max degradation for seven network configurations

configuration delivered almost identical survival times to the baseline. This finding is the basis of a cost-effectiveness analysis that could be planned for further research, based on which, one could select a topology with fewer valves, in order to reduce cost of acquisition, installation and maintenance, but without any compromise in effectiveness. As a result, the merits on survival times can be reshaped to time-based survivability estimates, where obviously the 32-valve configuration would be the most survivable configuration, for the given level of uncertainty.

The "restore" capacity investigation has revealed further variability across the different topologies for the four metrics of maximum degradation, recovery time, restoration offset, and average recovery rate. Figure 174 contains a comparison chart for the variation of maximum degradation with the increasing number leaks on the network. The 32-valve configuration experiences the smallest maximum degradation. It is interesting to observe that the variation with the leak number for each configuration has a unique shape. While the 32-valve topology degradation is continuously

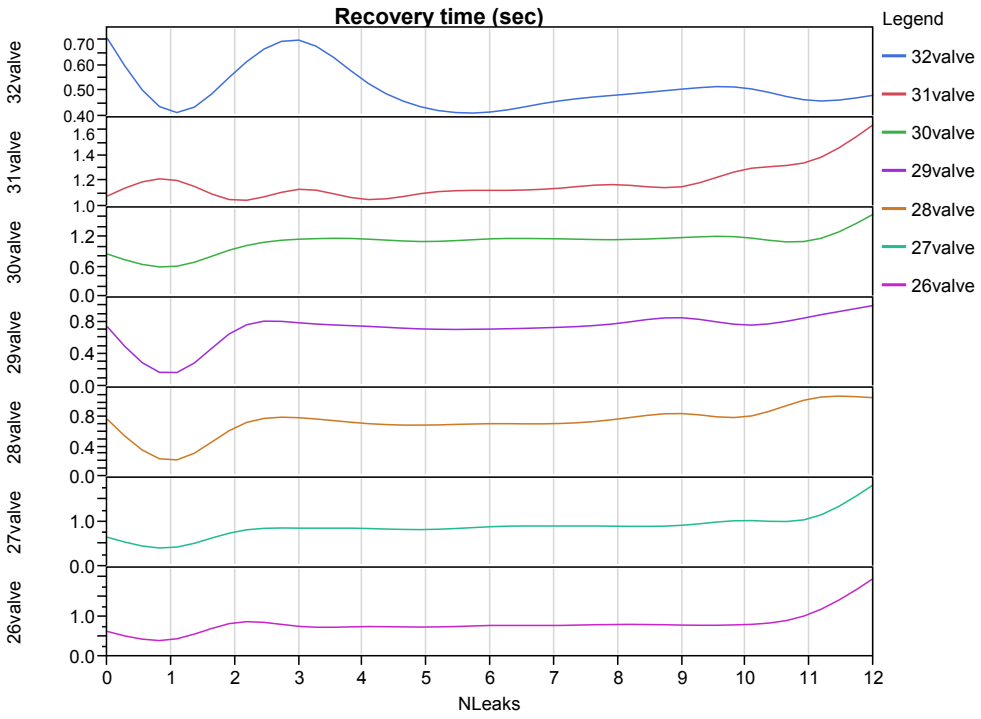


Figure 175: Recovery time for seven network configurations

and monotonically increasing with increasing leaks, the other topologies do not vary their maximum degradation monotonically. The 31 and 32-valve topologies are fairly insensitive to the leaks for a large part of the variation spectrum, except for the cases with 1-2, and 11 to 12 leaks. In accordance to the earlier result, the 29 and 28-valve topologies also demonstrate MC degradations close to that of the 32-valve baseline, further supporting the possible merits of a downsized topology that could be effective as the optimized baseline.

The recovery time comparison is shown in Figure 175. Once again, the baseline requires less time to recover, even though this time varies significantly between 1-5 leaks on the system. It must be noted that most of the observed variability in recovery measures, not only depend on the number of leaks or valves, but they are also affected by the choice of location of a valve, or the place that leak is observed. The 28 and 29-valve topology require slightly more time for recovery, even though that time is very close to that of the baseline.

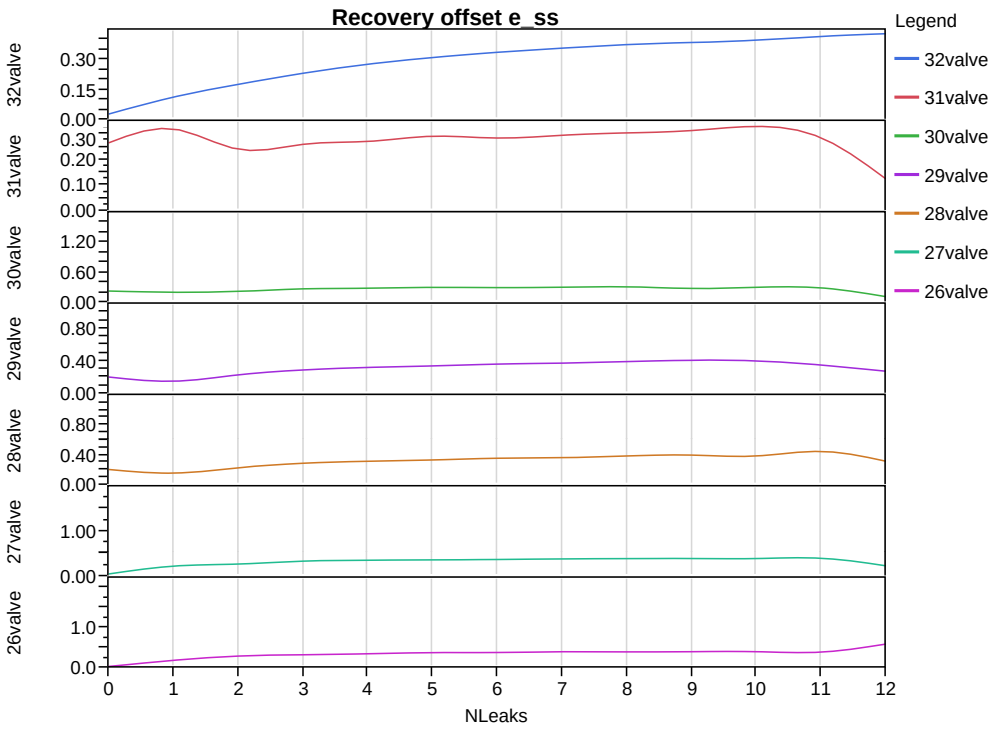


Figure 176: Recovery offset for seven network configurations

The restoration offsets after recovery is presented with Figure 176. For the 32-valve baseline, the offset is increasing with the number of leaks, while it remains as the only case where the offset is monotonously increasing. All other configurations follow a plateau for the range of 3-10 leaks. However, the offsets are ranging from zero to 0.45 of MC. Last, in Figure 177 the average recovery rate is presented. Except for the 30 and 29-valve configurations, the rates are fairly low, with a non-monotonic behavior for the baseline.

The final part of the comparative resilience assessment for the different cooling network configurations, are the capacity variations with leak number, for the "adapt" and the "absorb" functions. Figures 178 and 179 contain the mean values of the "adapt" and "absorb" capacity metrics RTO and D/T respectively. The overall offset from critical thresholds is the highest for the 32-valve configuration, implying that the system remains at capability levels closer to the ideal, no-leak response.

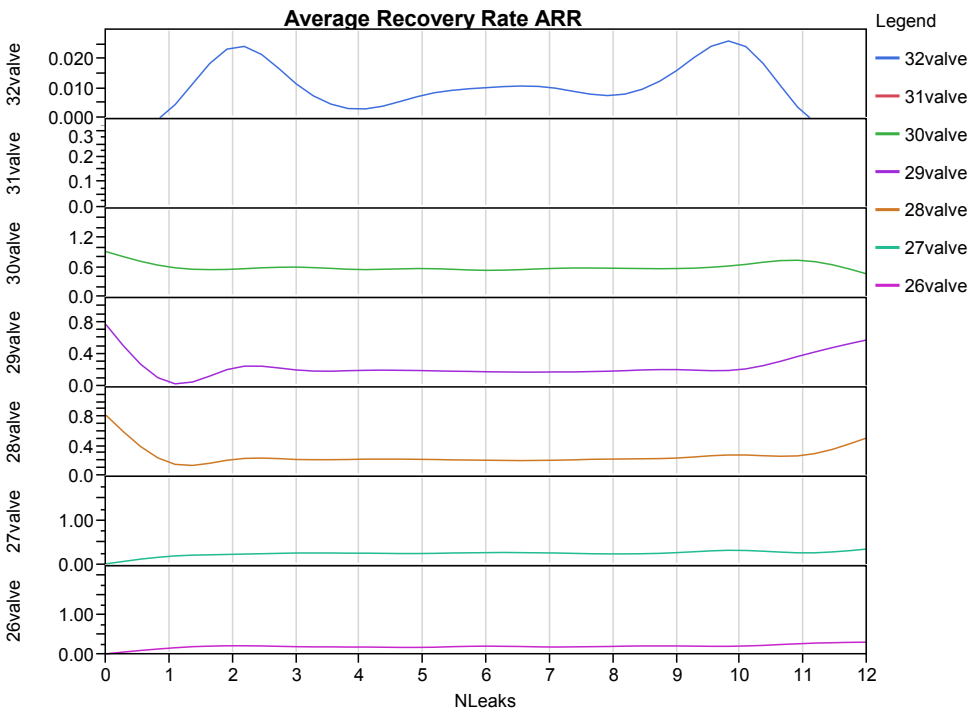


Figure 177: Average recovery rate for seven network configurations

Other configurations have scored lower RTO values, yet quite close to that of the baseline.

Larger variations are observed for the robustness related D/T metric. The ideal solution would return the lowest D/T, implying that the degradation effects for the input disturbance levels, are kept at low levels. Consistent to earlier observations on the comparably low MC degradations for the 28 and 29-valve configurations, the next lowest values after the 32-valve baseline are returned by the former solutions. The configurations with 30 and 31-valves have the worst performance with respect to their ability to "absorb" the effects of the leaks.

Using information from Figures 179 and 178, it is possible to define a design space for adaptability and robustness tradeoff investigation. It is based on RTO and D/T responses and it allows for discovering feasible solutions, when a set of adaptability and robustness constraints is provided. An example of the response diagram for

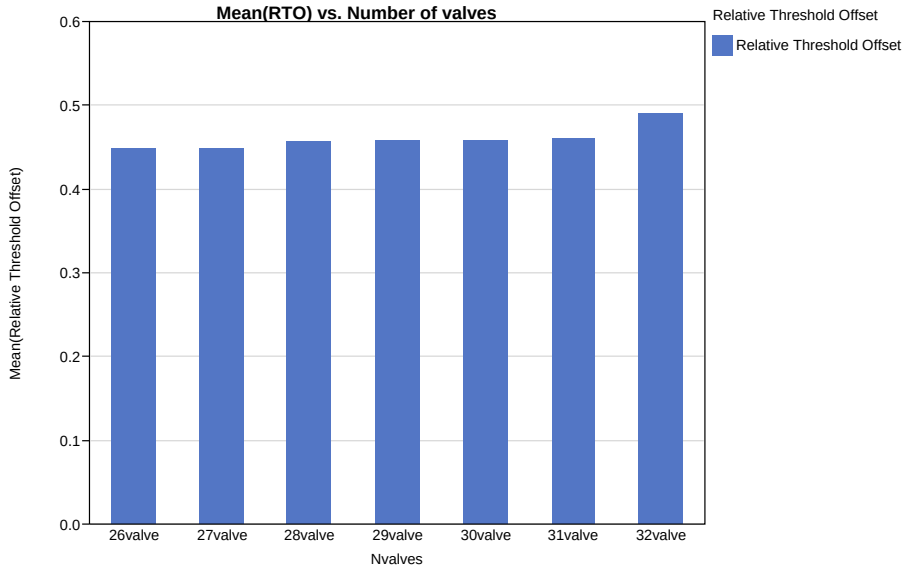


Figure 178: RTO for seven network configurations

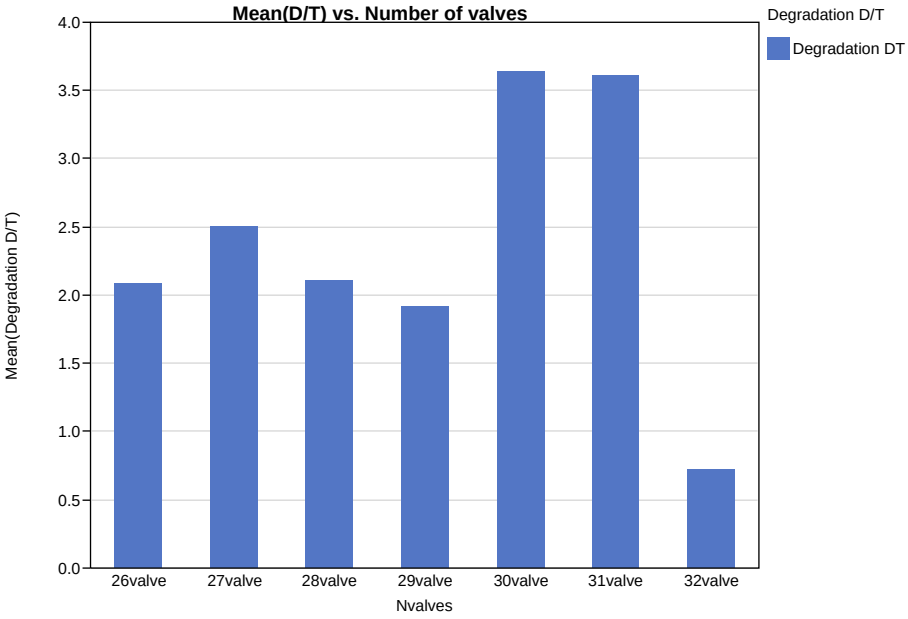


Figure 179: D/T for seven network configurations

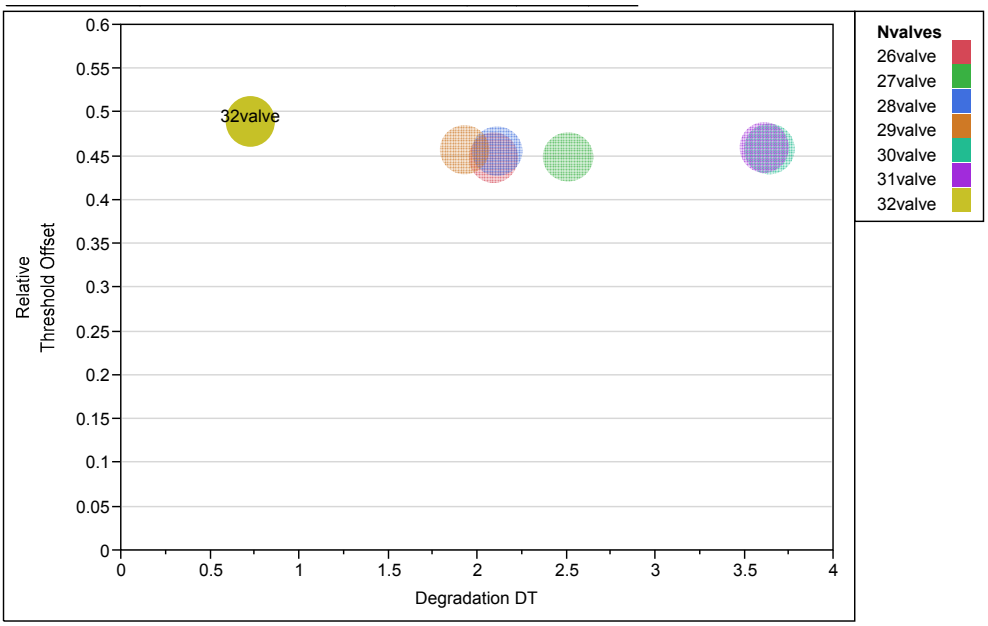


Figure 180: Response diagram with D/T, RTO for resilience-based design space exploration

design space exploration is shown in Figure 180, where each point represents a given configuration. The point coordinates are describing the capacities for the "adapt" and the "absorb" functions.

In a step further towards a resilience-based design methodology, feasibility of the solutions is explored, when adaptivity and robustness constraints become available. Then, all candidate solutions are evaluated with the resilience assessment technique, against given uncertainty scenarios. The assessment results are averaged and used as the source data for populating the design space. Imposing the design constraints, the response diagram of Figure 180 becomes the constrained design space of Figure 181. As an illustration example, for D/T no more than 2, and for RTO no less than 0.4, the feasibility test would return the 32-valve configuration as the most feasible solution. Additionally, the 29 and 28-valve configuration, also satisfy the feasibility criteria, yet marginally.

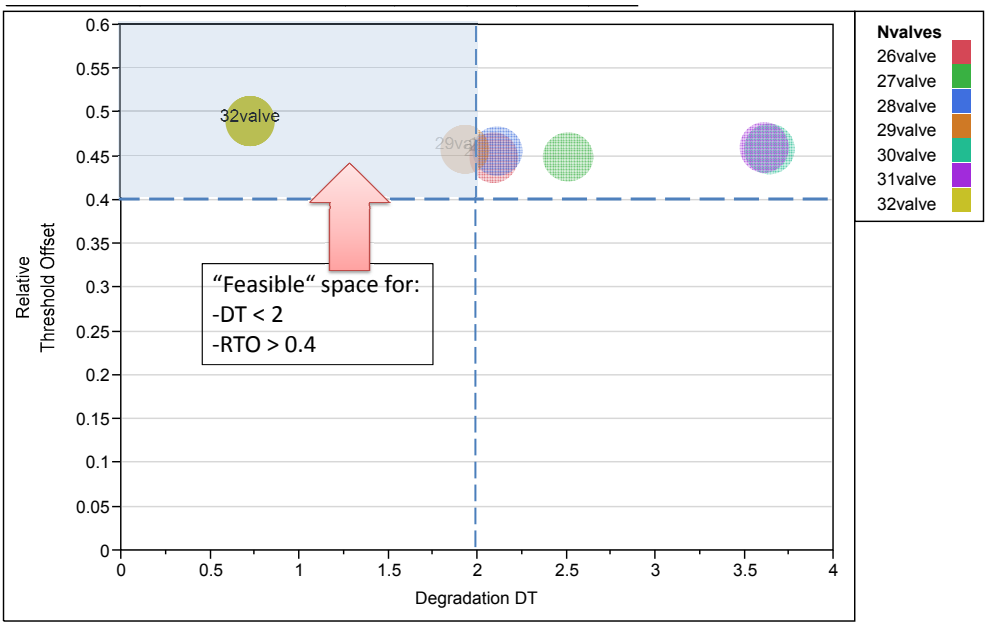


Figure 181: Response diagram with D/T, RTO for resilience-based design space exploration with constraints

6.4.2 Controller effects on resilience

Experiment 1.5 intends to demonstrate the effects of the controller on the recoverability and resilience capacity measures. According to the execution plan, the 32-valve system baseline responses are compared to the corresponding ones of the same architecture configuration, but without the ideal response controller activated. The controller is ideal, in the sense that it does not actually infer the locations of the leaks by itself through some analysis process, but instead it becomes aware of them, as part of receiving the scenario information as an input. This is not a realistic module, given that it automatically shuts the neighboring valves, when it receives the list of occurring leaks. As a result, the reliability of this comparative study has been question, yet however, the comparison study regarding resilience assessment for both configuration was performed.

Starting from the analysis of survival times, the distributions for both cases were identical. The configuration with the deactivated controller, has returned a mean of

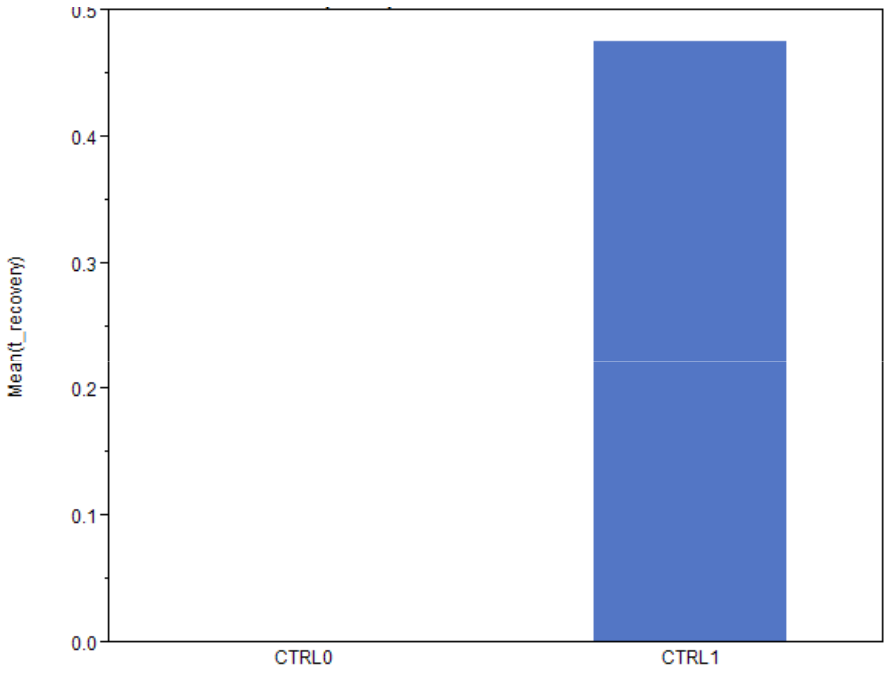


Figure 182: Recovery times for controlled and uncontrolled configuration

2.2 sec for survival time and 0 for standard deviation. The controlled configuration has returned a mean 2.195 sec with 0.072 standard deviation. The dispersity of data in both cases is minimal, and cannot guarantee the statistical quality of the further processing of results.

Another indication for the irregularity of the experiment, was the estimation for recovery times. While the controlled configuration did return a measurable distribution for the recovery time, the uncontrolled system returned a null distribution regarding recovery. Part of the responsibility for this behavior is the early termination of the system activity in a large number of cases, with the remaining ones to have the system unaffected in a non-realistic sense. Thus, the comparison for recovery time has returned Figure 182, where the non-controlled configuration did not gather any cases with any recovery process. As a consequence, a similar response has been observed for the average recovery rate ARR.

6.5 Summary of findings

With Chapter 6 , a complete resilience assessment study has been conducted for the 32- valve baseline configuration of the chill main system model. As the effectiveness of the assessment technique has been demonstrated, two studies were carried out, for the investigation of the impact of topology modifications, as well as the benefits of the rule based controller on system resilience. The former study, not only reaffirmed the optimized performance of the baseline configuration, it also allowed for quantifying the resilience capacity and performance differences from other valve configurations. The framework, has also showed its potential for supporting a resilience-based design methodology, through the exploration of the robustness-adaptability design space. Effects of the controller also supported the idea that intelligent control is an effective enabler for more adaptive, thus more resilient design configurations.

CHAPTER VII

CONCLUDING REMARKS

As a conclusion to this research, this last chapter provides a review of the original research objectives, along with the work that has been completed for addressing the research questions and supporting the hypotheses. Based on these findings, the list of the research contributions is presented and discussed. With a clear view of the contributions and their evaluation against remaining gaps on the research curriculum, it is possible to formulate the potential future tasks that would support the main research idea and further advance the development of the concept.

7.1 Review of research objectives

The present research efforts have been initiated by the need for more effective and survivable military or civil systems. In other words, the idea originates from the requirement that complex systems must be effective for the mission that it has been designed for, while maintaining mission capability and survivability, when exposed to an expected/unexpected set of external disturbances that affect its normal operating conditions. This requirement is the basis for Objective 1.

Several possible enabling concepts have been considered for supporting a solution to the previous problem. Resilience engineering is an emerging discipline, that is pertinent to safety management and provides a vision that could potentially address several open research opportunities towards the goal, implied by Objective 1. However, resilience engineering has not matured entirely as a discipline, thus there is a large number of open opportunities to be investigated. These range from definitions on resilient systems and resilient behavior to certain types of threats or disturbances,

evaluation frameworks, assessment techniques, and design methods that would support a resilience-based design initiative for complex systems. Ultimately, the main goal for the present work has been the development of a theoretical framework, upon which a resilience assessment techniques could be based.

7.2 Reiteration on research objectives

In this section, the main research objectives will be reviewed and evaluated based on experimental findings. The basic objectives have been summarized on developing a theoretical framework for resilience engineering, namely definitions, characteristics, requirements and applications for resilient systems, a resilience assessment methodology, and the demonstration of the methodology on a naval system application.

7.2.1 Theoretical background and framework development

The starting task for this research, underlined the need for system resilience to be redefined, along with the relevant attributes that a resilient system would possess. Resilience has been viewed in association to other safety management concepts, such as reliability, safety, survivability and security. Other aspects of resilience, according to the proposed definition have brought the corresponding degradation levels for mission performance ability and system health.

Part of the work has been primarily focusing on the understanding of resilience in materials science and structures, as well as how the current literature suggests the application of the concept in systems engineering. Resilience was mostly known as a characteristic of a structure, which highly depends on the selected material and design of the structure. An analogy can be drawn between the basic functions and behavior of an engineering structure against an engineering system. For instance, a structure that supports a load distribution of increasing amplitude goes through a series of thresholds that determine the level of degradation, up to the limiting state where the structure collapses. A similar scale and series of states for system collapse

can be devised, taking into account a system's equivalent degradation and propagation through recoverable/non recoverable states until system collapse. However, the current status of implementing resilience in systems engineering is still at its infancy stages. In particular most experts have described how a resilient system must behave and what its basic functions are, yet it is still unknown how such a system can be implemented or even if they are feasible overall.

Thus, as part of the contribution to bring resilience engineering in the conceptual design of a system, a metrics framework has been defined and further developed to support a methodology for system resilience assessment. This method, along with the accompanying metrics carries many similarities to existing metrics and risk assessment techniques. Yet, it is centered on the concept of resilience, seeking to address how effectively a system can perform the necessary functions that would allow one to classify it as resilient.

For the development of the framework, a multi-spring-mass damper system model has been used, with a controller wrapped around it. In order to capture all the envisioned attributes of a resilient system, several assumption were made regarding the SMD model, for the purpose of both simulating and emulating the behavior of a true resilient system.

7.2.2 Probabilistic resilience assessment technique

With the probabilistic technique, the capability of a system to adapt, absorb change effects and restore itself after a given set of possible disturbance condition combinations is evaluated in a transparent way, that is consistent to the resilience definitions. All systems carry certain capacities to perform these functions by design, yet one of the objectives was to investigate how these capacities vary not only with uncertainty, but also with design or reconfiguration strategy change, while the system is operating on its mission.

Clarifications on the definitions for safety, survivability, robustness, adaptability and resilience have been discussed, and their association has been investigated through experiments. Mission uncertainty was analyzed and modeled through multiple factors. Capacities for the three resilience function were compared and their correlation was examined. Last, topological or logical changes on the controller were evaluated with the derived metrics and trends were investigated and linked to the system's physical behavior. Last, as part of fulfilling one of the earlier objectives, the relationship of system resilience to survivability was investigated as, certain enhancement solutions would improve the system's capacities and furthermore return longer life times, hinting for more survivable systems.

One of the challenges that have arisen, mostly due to the nature of the problem, was the possibility of modeling an entirely unexpected scenario case. Remember that according to the resilience definitions, a system is expected to be able to withstand not only expected but somewhat uncertain disturbances on their deployment, but also it should manage to have a reasonably favorable response when affected by a never seen before disturbance. That requirement is beyond the scope of this research to address and can be a noteworthy proposed idea for future work.

7.2.3 Demonstration of the resilience assessment on a naval system architecture

The last objective is to demonstrate the applicability of the resilience assessment technique to a naval architecture problem. For the method to be applicable, certain requirements were in place for the two problems, in terms of their dynamic responses and the availability of dynamical system time histories. The same set of research questions (RQ 2, 3) was in place for the demonstration, and the research hypotheses have been explored for the larger scale naval system. Additional comparison studies, between the alternative architectures has revealed the benefits on survivability, recoverability, and overall resilience, in accordance to the proposed definition.

7.3 Research Contributions

After reviewing the research objectives that have initiated this research and evaluating how well the expectations were met, it is important to clearly identify the contributions that have been made to the field of resilience engineering through this particular research effort. Part of this would be to describe how the achievement contributes to the current state of the art, given that the state of the art has already been identified through the literature investigation presented in Chapters 2 and 3. As both the SoA and the proposed method have been documented, the advantages of the new method over the established methods are discussed. Last, other aspects of the benefits of this research are outlined, such as the practicality of the method, scalability and its readiness to be used in larger scale complex systems in the real world.

7.3.1 Summary of contributions

The key contributions of this research to the SoA for system resilience assessment are summarized in the following:

- Definition of system resilience. Not only a complete definition of what a resilient system is but, there was also a discussion of how resilience as a safety management concept relates to other safety management concepts, such as survivability, reliability and security.

- Complete resilience assessment framework. Moreover, this definition was taken further to produce a list of envisioned resilient system attributes. These attributes were the basis of the three basic functions that a system must be able to perform for being resilient. Eventually, based on that set of functions and attributes, the necessary resilience measures have been formulated.

- Resilience assessment method. With the resilience measures as the basis, a

range of higher level and aggregate measures was obtained for a given system baseline. This method is useful for quick comparisons of varying architectures when subjected to a given scenario. Equivalently, a fixed architecture can be subjected to a range of different scenarios, allowing for assessing its resilience, mostly from a solution robustness and adaptability perspective.

- Demonstration of survivability improvements with more resilient designs. This contribution implies the extension of the deterministic resilience assessment method to become a probabilistic analysis for resilience. This allowed for seamlessly integrating the measures of system resilience, when the system is experiencing a chain of events that impose change on its normal operating conditions, to survivability contributions and thus to overall system survivability.

- Simple problem demonstration. In order to develop the methodology and the resilience framework before this, a canonical small scale problem has been devised and implemented. Thus, the canonical problem has been a physics-based simulations that emulates the behavior of resilient system, as closely as possible, in order for the lower level measures to return nonzero or nontrivial values.

- Assessment of a scaled-down naval system. Last, the full scale probabilistic assessment method has been demonstrated on notional small scale YP ship cooling network. With this contribution, not only the applicability of the method on a practical problem is demonstrated, but a case is made for its scalability and flexibility to be used for any large scale complex system that behaves dynamically and is experiencing certain changes on its mission and overall health.

Besides the contributions on the research curriculum, there has been a number of technical contributions. these are:

- A complete JMP script suite for response analysis and supporting visualization for the resilience assessment method.

- Scenario DOE generation procedure
- The SMD implementation in Simulink.
- Enhancements and added flexibility on the integrated Java-Simulink model for the naval system architecture.

7.3.2 Foreseen and unforeseen research questions

Except for the addressed research questions, that have been supported by a set of hypotheses, based on experiment findings, several new research questions have emerged, mostly pointing towards the direction that this research is expected to take. Some these questions are:

- Is there a more generic and multi-purpose scheme for the resilience assessment metrics?
- How can reconfigurability and adaptability effects be better modeled and evaluated?
- As advocated in chapter 5, system adaptability could possibly manifest itself through dynamically changing critical threshold, how could such functionality be implemented and properly evaluated?
- How can the probabilistic resilience assessment method be extended to become an integrated part for resilient systems design?

Most of these questions were foreseen, yet any attempt towards addressing them would be out of the scope of this research. On the other hand, such questions could definitely be a good starting point for research opportunities to be explored in the future.

7.3.3 Practicality and importance of findings

One of the guidelines for developing the method, was the comprehensibility that it should carry for non-specialists to understand and follow. The key concepts around system resilience and the proposed functions that support the four resilience capacities carry a high degree of generality. this allows for the concept to be applicable for any engineering system, and also for non-engineering systems as well. Given that the raw simulation model is only required to provide dynamic data on system degradation regarding mission performance ability and system health, this allows for the method to be applicable for any complex dynamic system that can provide such information.

7.4 Recommendations for future work

This present research has been a remarkable example of how gaps in the state of the art and open research questions can lead down to a path, where the start and end points share so little in common. With the need for designing more effective systems, the major first checkpoint towards addressing the problem, has been the need for designing more survivable systems, under the expectation that increased survivability always make a military of civil large scale system more effective. Extensive background literature search has revealed the State of the Art in survivability based-design techniques across multiple engineering and scientific domains. Most approaches offer a great set of options for formulating requirements for survivable systems, assessing survivability of given system architectures and suggesting multiple design enhancements.

At the same time, resilience engineering has been introduced to provide alternative ways of understanding and analyzing the problem, however, this action brought more challenges on a problem that is already of high uncertainty. While resilience has been a very suitable concept to address the problem, it represents a new, emerging field that has its growing dedicated scientific community that is still exploring the concept

from quite diverse perspectives and for a multitude of applications. In other words, it is only the onset of the proliferation of resilience engineering as a scientific field and there are no standard definitions, metrics, assessment methods, or relevant system design methodologies with system resilience as an objective function. This research has concentrated on conducting a thorough SoA investigation on progress made by the community on the above fields, and proposing a set of metrics and definitions for supporting a system resilience assessment methodology. However, many opportunities for extending this effort to the level of a systems engineering-based design methodology have arisen.

The first opportunity has been the idea of developing and proposing a unified generalized metric and evaluation framework. In other words, work that is presented with this research is extended to become a general procedure for a larger range of complex dynamic systems. This framework would enable multi-domain design procedures for increased system effectiveness and resilience. With the inherent design uncertainty in complex systems design, a physics-based Modeling and Simulation (M&S) environment has been considered as a necessary tool for scenario-based design evaluation.

With an effective resilience assessment method, the following logical step is to guide the research towards an advanced system design methodology. However, at this point one could question whether the traditional design methods can be adequate for accommodating resilience as a design objective. One may wonder for instance, how the traditional GAP analysis and design space exploration should be modified to account for the highly dynamic and uncertain nature of the problem. A great uncertainty is also apparent regarding all possible design changes that must be applied (technology addition, system architecture modification, etc.) at each design cycle in order to achieve the performance targets. Finally, to reach the goal of delivering a complete design methodology that is objective and repeatable for any set of initial stakeholder requirements, all possible and applicable decision making techniques need

to be investigated, ensuring their effectiveness on highly dynamic and complex systems. Along the path of investigating and building the building blocks for the method development, the following research opportunities have been identified:

- Design space exploration with resilience analysis
- Investigate and model technologies for enhancing system resilience
- Include control system design as a possible adaptability enabler
- Resilient concept development and selection

Some of the key disciplines and research areas that one could potentially be relevant to the previous directions are control theory (nonlinear, adaptive and robust control for enabling adaptability and intelligence), safety engineering and survivability-based methods (risk and survivability assessment, limit analysis, safety oriented technologies), as well as damage modeling, health modeling and uncertainty modeling

7.4.1 Design space exploration with resilience analysis

With the above model augmentations underway, it will be possible to explore the architecture design space, in conjunction to the control design space. The main proposed design exploration tool for system resilience is the Mission-Health trajectory plot. However, to bring more emphasis on the resilience aspect and have an additional layer of detail, a 3D plot of resilience function representations can be constructed. With the resilient behavior assumed to be expressed through the other three functions, "adapt", "absorb" and "restore". To narrow this scheme further down, "absorb" is more representative of the system's robustness levels. "Restore" is more of an outcome that can depend on both "absorb" and "adapt" functional capabilities. Thus, the function that reflects better the system's resilience and can be the distinguishing factor is hypothesized to be the "adapt" function. The aforementioned 3D plot, will not only be used a design utility, but also as a means of investigating the relationship

between system restorability and its ability to absorb the effects of change and adapt to change respectively.

7.4.2 Investigate and model technologies for enhancing system resilience

At the point that the resilience assessment framework is complete, along with the assessment method, one can investigate what reconfiguration strategies in combination with what selected design configuration can return a design that is more resilient to a set of threat scenarios. Using the canonical problem to illustrate this objective, what combination of springs and dampers would be required, with what count of redundant switchable springs and what reconfiguration strategies (algorithms for enabling redundant springs) is the equivalent problem statement. The naval system investigation would include combinations of smart valves, regular valves and control algorithms.

7.4.3 Resilient concept development and selection

At a later stage of this research task, decision making techniques in conjunction with Monte Carlo simulation should provide the basis of extending the resilience assessment technique to a methodology for designing more resilient systems.

APPENDIX A

INTRODUCTION TO SYSTEM EFFECTIVENESS

A.1 Defining system effectiveness

The importance of system effectiveness in systems engineering has been underlined through military doctrine. Given that a *mission* can be defined as the "ultimate output of a system" [138], military doctrine describes the qualities of a military system, in order to be able to accomplish multiple missions successfully in a multiple threat environment. Figure 183 lists key doctrine highlights towards system effectiveness. Except for military doctrine, the definition of a system in engineering also hints on system effectiveness. For instance, a definition for an engineering system is focusing on its operating functions, which are the key elements for mission effectiveness [218]:

"A system may be considered as constituting a nucleus of elements combined in such a manner as to accomplish a function in response to an identified need. A system must have a functional purpose, may include a mix of products and processes, and may be contained within some form of hierarchy."

To better understand the concept of system effectiveness, the literature has revealed a great diversity in definitions and applications. Soban and Mavris [218] have acknowledged that system effectiveness holds different meanings for different communities and applications. In most cases, definitions are based on domain-specific terminology, including system-dependent effectiveness metrics. A common key characteristic across applications, indicates that effectiveness is linked to basic system objectives and mission requirements. Mission requirements are indicative of overall mission objectives and system expectations. Goode and Machol [92] were one of the

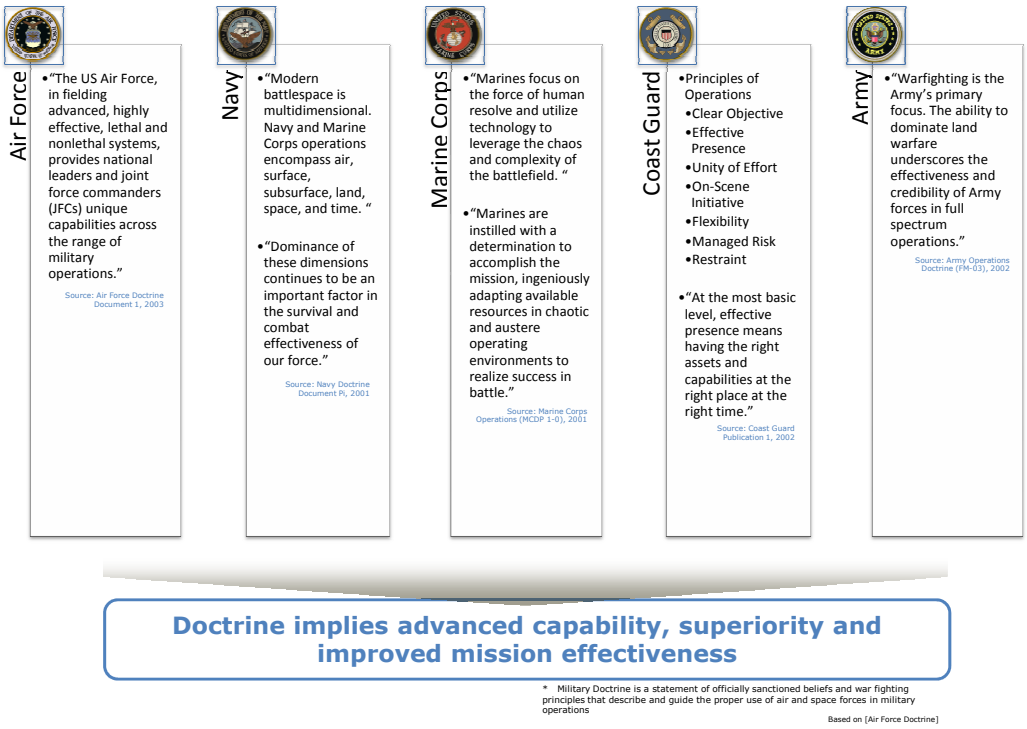


Figure 183: Doctrine of the U.S. Military forces

first authors to provide a definition for system effectiveness, simply stating that:

"effectiveness is the criterion by which solutions will be judged proposed solutions, solutions under test, or solutions in being"

Other definitions of effectiveness in different domains are presented in Figure 184. Goode and Machol also developed a set of desired characteristics that lead to the *Measures of Effectiveness* (MOEs). At the same time, several researchers and organizations have attempted to introduce a set of standard measures for system effectiveness that could be applicable across multiple engineering domains. A standard definition is expressing effectiveness as the product of three probabilities [97]:

$$Effectiveness = p_{Availability} \cdot p_{Dependability} \cdot p_{Capability} \tag{79}$$

Availability is a measure of the system condition at the start of a mission and is a function of the relationship among hardware, personnel and procedures [97].

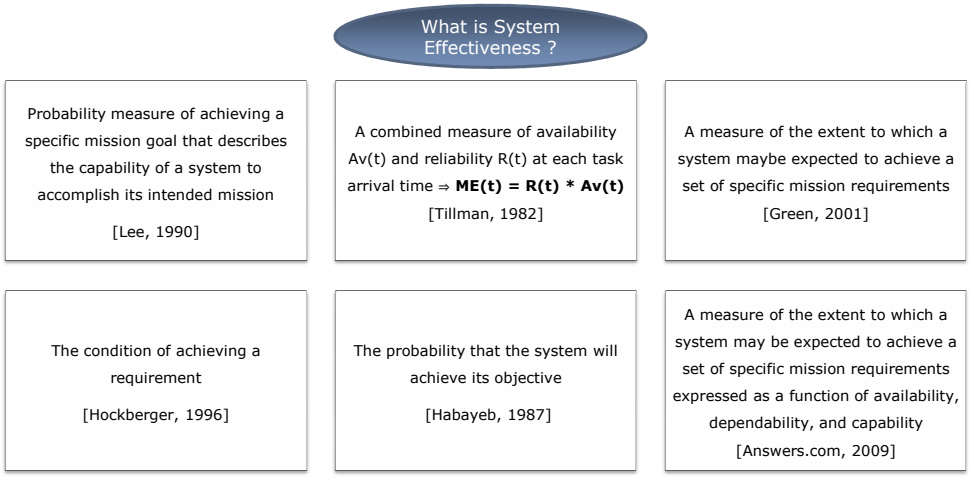


Figure 184: Definitions for System Effectiveness

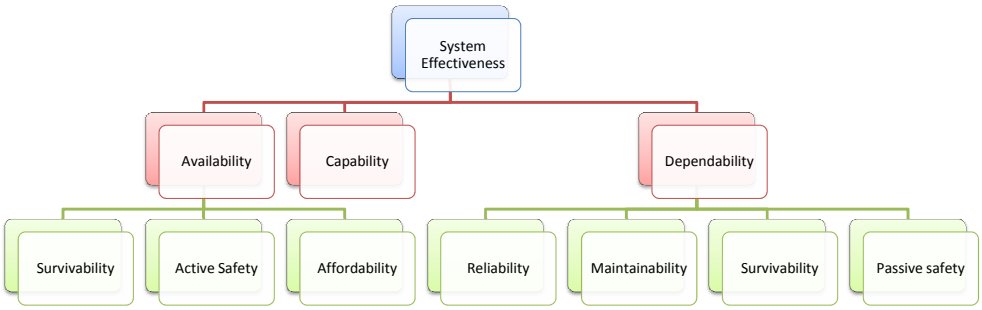


Figure 185: System Effectiveness breakdown [97]

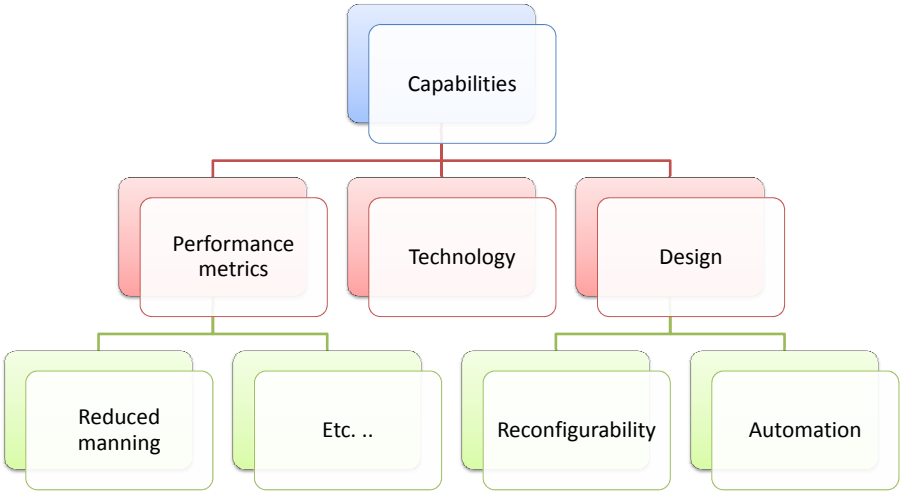


Figure 186: Capability breakdown [97]

Dependability is a measure if the system condition at one or more points during the mission. In most definitions, dependability can be broken down to survivability, reliability, maintainability, operability (readiness) and repairability [97], as shown in Figure 185. Capability is a measure of the ability of a system to achieve the mission objectives [97], and can be further broken down into other related "-ilities" as shown in Figure 186.

A.2 Observations on system effectiveness

Further exploration of system effectiveness for different application, has lead to a number of facts, which are outlined in Figure 187, and discussed in the following sections.

A.2.1 System effectiveness is a probabilistic measure

With threats that could emerge under highly uncertain system operating conditions in the mission environment, along with the changing system requirements, a probabilistic approach is necessary for addressing mission uncertainty in system effectiveness estimations [155]. Such observation was originally made by the 1964 Weapon System Industry Advisory Committee (WSEIAC), with a report that addressed the problem

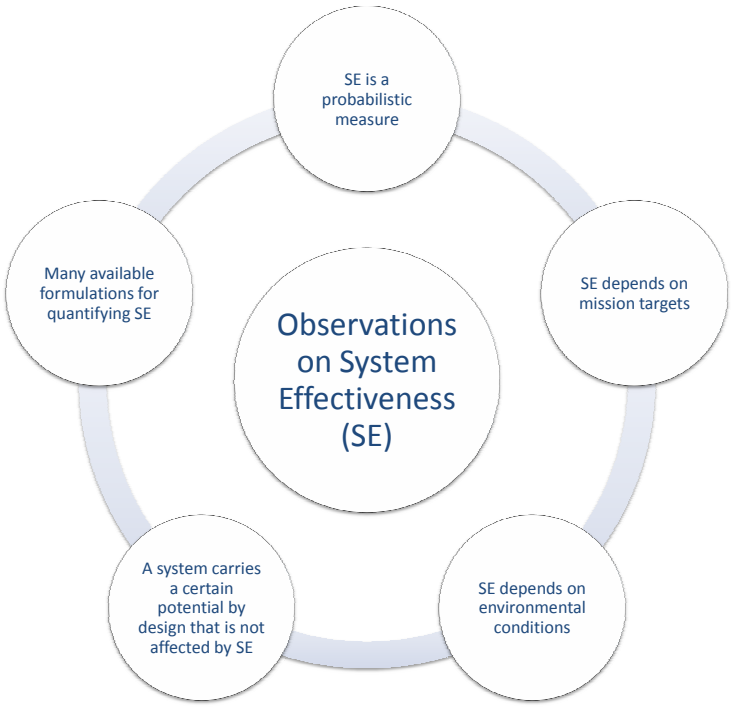


Figure 187: Observations for System Effectiveness

of systems effectiveness [200]. The WSEIAC introduced a definition, which opened the way for probabilistic methods as enablers for system effectiveness evaluation.

Most effectiveness definitions focus on how successfully a system can achieve its mission requirements [94], [105]. With mission uncertainty being a critical factor on system effectiveness, most formulations are probabilistic, in order to account for operational risk [138]. Based on Rudwick's literature review, Ackoff has also been suggesting that system-of-systems (SoS) effectiveness is also evaluated through probabilistic approaches [3].

A.2.2 System effectiveness is assessed against goals for successful mission completion

Given that a mission is defined according to a set of objectives, system effectiveness is assessed through metrics that compare time dependent responses to goals set by the mission objectives. Under this direction, the Military Operations Research Society's

(MORS) has performed a set of studies for quantifying mission goals and measures for system effectiveness [94]. Similar efforts have been documented by the WSEIAC committee.

A.2.3 System effectiveness strongly depends on changing environmental and mission conditions

As McManus et. al indicate, a system is required to operate under varying external or internal conditions, which could induce endogenous (generated and propagated within the system inner structure), or exogenous (generated or caused by external factors) changes on the system [155]. Changing environmental conditions (context) are strictly exogenous, while physical system changes are typically endogenous.

Based on the earlier observation, McManus et al. have viewed system effectiveness or ultimate success in relation to three primary factors [155]:

- **System expectations (Needs)**: Changes in needs may include increased expectations on the system (a demand for higher levels of the same service) or changes in the metrics of success (some new function is demanded of the system). Changes in expectation can be either endogenous (system reconfiguration) or exogenous (stakeholder requirements).

- **Development and operational environment (Context)**: Changes in context are usually external constraints on the system: it must operate successfully in the new context. Context related changes are strictly exogenous.

- **System form (System)**: Changes in the system form may include subsystem reconfiguration or component deterioration, malfunction, partial operation or total failure/activation. Further identification of inner system limitations that can trigger system form changes can be based on *system partitioning*, introduced and thoroughly discussed by [97]. This latter type of change strictly belongs in the endogenous changes grouping.

A.2.4 All systems demonstrate a certain capability for performing their mission

While being aware of possible changes in needs and context, designers cannot accurately predict what changes will occur and at what timing on a system's life cycle. Change in mission expectations and in environmental conditions is a major source of operational uncertainty, on which a designer has no influence. System designers typically only have influence over the system's design, which determines its performance and its capability is optimized, subject to assumed levels of operational uncertainty [198].

Recent efforts in systems engineering have advanced the state of the art in *capability-based design*. Capability-based design is pre-defining the system performance effect (or system capability) and investigates the solution by generating all possible design alternatives and selecting the optimal (subject to the particular problem constraints and requirements) that can deliver the same capability [24]. However, similar approaches can ensure that the system has the desired built-in capability for performing multiple missions and tasks, assuming that it can always withstand threats emerging in its operational environment. Thus, a capable system is an effective system, in the sense that its built-in capability is maintained, while experiencing threats, attacks or other possible mishaps during its mission.

A.2.5 Several formulations available for quantifying system effectiveness

One of the most prominent approaches for analyzing system effectiveness, is the method proposed by the *Weapon System Effectiveness Industry Advisory Committee* (WSIEAC) in 1965 [21]. The WSIEAC model is based on the enumeration of the significant system states over the entire mission. By *system states*, it is implied that there are discernible conditions of the system which result from events occurring prior to and during the mission. A state at high level can consist of combinations of states at a lower level. For instance, a state can be the condition at which a system

is available and operable, namely a state in availability and a state in operability can comprise a state at the system level.

A system can transition through different states during a mission. According to Equation 79 that defines system effectiveness, the structure of the equation with the possible states can be expressed as:

$$E = [A] \cdot [D] \cdot [C] \tag{80}$$

where $[A]$ is the availability row matrix, $[D]$ is the $n \times n$ matrix of dependability and $[C]$ is the capability column matrix. It follows that equation 81 becomes:

$$E = \begin{bmatrix} a_1 & a_2 & ... & a_n \end{bmatrix} \cdot \begin{bmatrix} d_{11} & d_{12} & ... & d_{1n} \\ d_{21} & d_{22} & ... & d_{1n} \\ ... & ... & ... & ... \\ d_{n1} & d_{n2} & ... & d_{nn} \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \\ ... \\ c_n \end{bmatrix} \tag{81}$$

Each element a_i, d_{ij} and c_j represents the corresponding figure of merit for every element j at each availability state i. These figures of merit can be calculated by the metrics of the *MORS* framework. There are different approaches in the selected sets of metrics for describing effectiveness, strongly depending on the system point of view. System effectiveness at the mission or the campaign level is typically measured by numbers or percentages of systems killed/survived in battle. At the system level, the focus shifts towards individual events and characteristics such as type of system, type of attack, vulnerability, casualties, and recovery time.

Hootman [112] has conducted an extensive literature survey on the subject of *Measures of Merit* (MOMs). The latest and most prominent effort for a a single, consistent description of a MOMs system, is attributed to the WSEIAC initiative [21] by the MORS society. System effectiveness is being broken down in sets of contributing metrics that reflect the behavior of the architecture at different and bounded levels. The breakdown is shown in Figure 188.

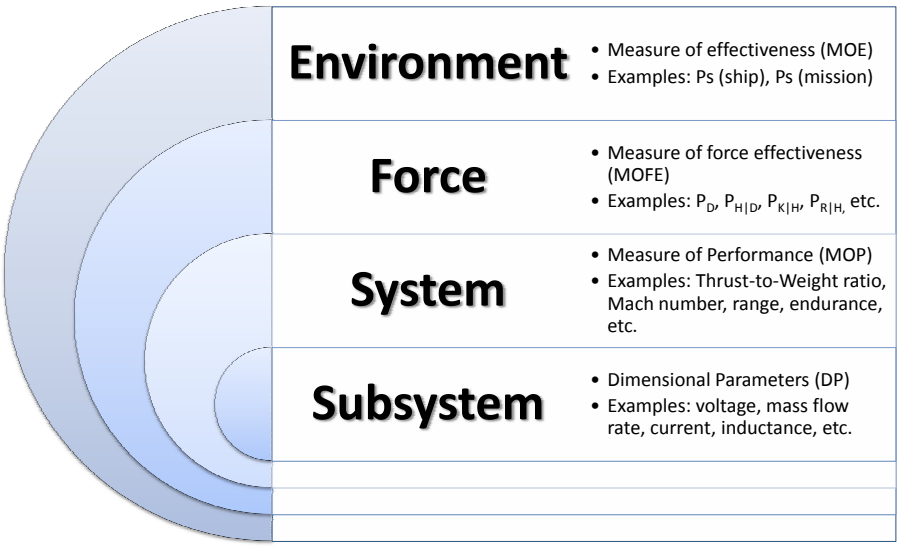


Figure 188: System Boundary Levels [94]

The MORS approach work concerning the measures of effectiveness is summarized below:

- **Dimensional Parameters (DP)**: The properties or characteristics of the physical entities whose values determine system behavior and the structure under consideration [94].

- **Measures of Performance (MOP)**: MOPs are non-probabilistic measures of performance [112], related to inherent parameters (physical and structural) and measure attributes of system behavior [94].

- **Measures of Effectiveness (MOE)**: MOEs are a measure of how the system performs its functions within an operational environment [94]. MOEs are metrics that measure the degree of effectiveness attained in a achieving a requirement [105].

- **Measures of Force Effectiveness (MOFE)**: MOFEs are a measure of how the system, and the force of which it is a part, performs its missions [94]. MOFEs

may also be referred to as measures of system effectiveness (MOSEs), or as an overall measure of effectiveness (OMOE).

- **Measures of Merit (MOM)**: MOMs refer to all measures that characterize a system, incorporating all measures that characterize a system [94]. As the definitions indicate, MOMs develop in a very hierarchical manner.

The effectiveness equation can be transformed to a reduced form according to the type and mission of the system under study. For instance, concerning a non-military system with a certain capability level, aspects like readiness or reliability become more important than survivability or stealthiness, therefore Equation 79 is reduced to include only reliability and operability under dependability. All other terms are fixed and do not contribute in the variability of system effectiveness. An example of a reduced version of Equation 79 has been given by Lee et al., where system effectiveness is defined as a combined measure of availability $Av(t)$ and reliability $R(t)$ at each task arrival time [138]. It is mathematically given by:

$$SE(t) = R(t) \cdot Av(t) \tag{82}$$

Equation 82 is introducing time t as another important factor in the effectiveness measure, thus implying that several changes can occur within the operational environment of the system, threat or non-threat related. A system is required to perform several tasks which arrive randomly during the fixed mission duration, while having only two states of operation, either remaining "on" or "off". Additionally, successive times in the on-state and in the off-state are statistically independent. Another assumption refers to the correlation between the components of system effectiveness. In a complicated or complex system, it is expected that reliability and availability are correlated, and the same can be argued for capability. For equation 82, it has been assumed that there is no correlation between reliability and availability. In

general however, it is not always the case that system effectiveness is determined by independent events and contributions.

Switching to an alternative formulation of measuring effectiveness, the Air force Research Laboratory (AFRL) have introduced a probabilistic approach for this purpose. It relies on performance-based measures, taking into account the mission objectives and probability of success criteria, as well as system performance under damage propagation that is estimated through companion damage and fail prediction models. System effectiveness SE in this context is given by:

$$SE = P(SE) \cdot (Consequence) = [P_A \cdot (1 - [P_I \cdot P_N])] \cdot C \tag{83}$$

where P_A, P_I and P_N are the probabilities of attack, interruption and neutralization, and C is a measure of the impact of damage or fail consequence on the system.

The U.S. Navy has developed their own framework for evaluating system effectiveness. A good discussion of this framework is provided by Hanifan et al., through the naval system effectiveness manual NAVMAT P3941-B [101]. As Habayeb also argues, system effectiveness is broken down in availability, dependability and capability. Effectiveness for naval systems is measured by the *Index of navy defense effectiveness* E_d. It is expressed by:

$$E_d = \frac{W \cdot E_s}{E_t \cdot (C_a + C_o)} \tag{84}$$

where E_s is the system effectiveness, E_t is the index of time effectiveness (system degradation over time), W is the military worth of the system's mission, C_a are the acquisition costs, and C_o are the mission and system operating costs. It must be remarked that is the analysis refers to multi-year multi-mission operations, then military effectiveness and costs should be estimated on a year basis per mission assignment.

System effectiveness E_s is estimated as shown by Equation 85:

$$E_s = \int_0^\infty F(x)g(x)dx \tag{85}$$

where $F(x)$ is the probability that a system's performance is at least x and $g(x)$ is the probability that the demand level is x. If performance ability and demand happen to be interrelated, then a modified version of Equation 85 redefines E_s as:

$$E_s = \int_{x=0}^{\infty} \int_{y=0}^{\infty} u(y|x) f(y) g(x) dy dx \tag{86}$$

where E_s is calculated based on the premise that success may be attributed to performance less than demand levels, $f(y)$ is the probability density function of performance level being y, and $u(y|x)$ a utility metric indicating the performance level of y when demand level is x.

APPENDIX B

METHOD EVALUATION CRITERIA

As part of the research benchmarking process, it is necessary to qualitatively evaluate the SoA approaches that have been identified through the literature search. Findings include definitions, methods and techniques across multiple scientific and engineering domains, returning a diverse collection of technical approaches. However, for the current dissertation, two types of safety management approaches are of interest, design methods for safety and survivability, as well as assessment techniques.

A set of criteria for evaluation and comparison of SoA methods for each type of method is suggested. The purpose of this exercise is to identify the strengths of the techniques and investigate the contribution potential to current open challenges in safety engineering. The evaluation criteria for method and technique features are based on practices and comments found on the relevant literature resources. They are grouped under three basic themes, namely method fundamentals, method features and method applicability, and are summarized in Figure 189.

B.1 Fundamentals

As discussed earlier, the three *fundamental* method ingredients are the metrics and evaluation framework, the assessment methods and the enhancement strategies, all defined as follows:

- **Metrics and evaluation framework**. To design for safety or survivability, the method must provide the framework for evaluating a configuration against the design requirements. In most cases, the step that is assessing survivability is the part where this evaluation occurs. However, to execute the assessment,

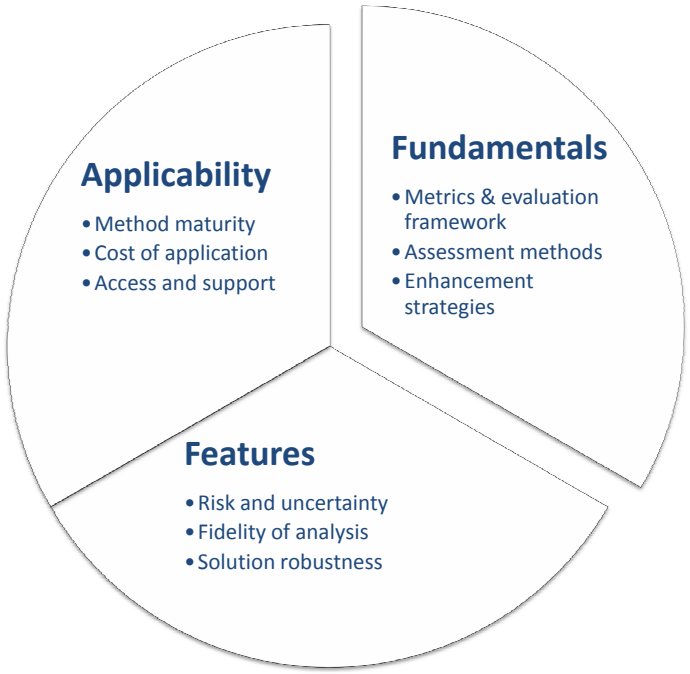


Figure 189: Evaluation criteria for Survivability-based design methods

it is necessary to have the theoretical framework of metrics and relationships for the calculations defined. Despite the fact that each one of the methods follows their own approach with a specific set of metrics, one would observe that processes and metrics are similar or equivalent. For instance, power system engineers often refer to "operability" [225], while naval engineers use the Quality of Service (QoS) [65], two survivability related metrics that are pretty similar.

- **Assessment methods**. Safety or Survivability assessment for the types of methods discussed is the equivalent of testing and verification, or the design phase, when a current design configuration is evaluated against the minimum safety requirements. It is the essential core of any survivability engineering approach, as a separate method evaluation session is conducted and presented in the following section. Literature is abundant on assessment techniques, yet there is a common subset of steps and procedures for SoA techniques, as it has been observed.

- **Design enhancement strategies**. The results of the assessment often reveals design weaknesses and safety gaps. Engineers then closely examine the shortcomings of the design, and try to understand what needs to be improved. As the literature search demonstrated, there are several strategies in the form of design techniques or technologies for improving survivability.

B.2 Features

Moving on with the *method features*, this is a set of criteria that underline additional strengths and benefits of the method, which sometimes become mandatory according to the nature of the system or the problem. For instance, if the system is expected in a highly uncertain environment, the design method must then account for operational uncertainty. If the system is an unconventional design where no historical data could be reliable for the assessment, then possibly a physics-based modeling approach would offer more realistic insight. Last, advanced design methods seek for the robust, rather than the optimal solution, and given the possibility of improving survivability through resilience, which to some extent is equivalent to robustness, then the latter is another favorable criterion for the method. The following criteria are thus considered for the methods:

- **Risk and uncertainty considerations**. Due to the inherent operational and design uncertainty, the system's mission capability and survivability, are changing and usually do not match the design expectations. Methods for system acquisition must address this critical issue, by ensuring that a design will perform within a frame of expected behavior for given range of mission and environmental uncertainty. Safety and survivability engineering regulations are heavily concerned on operational risk du to the presence of this uncertainty (e.g. SOLAS criteria, JTCG/AS, OPNAV P-86-4-99). Certain probabilistic

and stochastic approaches and formulations can assist in identification of uncertainty sources and risk.

- **Modeling fidelity**. Most current design practices make use of legacy codes or trusted computational models to run computational experiments, without the burden of expensive and time consuming prototype testing, at least in early conceptual design phases. In some cases, unconventional concepts could require high fidelity experimentation for increased modeling accuracy to reduce the uncertainty on a configuration that has never been tested or maintained before. Historical data, even if available would certainly not offer accurate insight on a revolutionary concept. Physics-based *Modeling and Simulation (M&S)* is becoming a standard in industry and academia, for developing simulation tools for analyzing and evaluating innovative design solutions and architectures.

- **Solution robustness**. In the conceptual design phase, a robust solution refers to a system design configuration that has been optimized to be more insensitive, in terms of its response to either expected or unexpected disruptions during its typical design mission [154]. In a traditional feasibility study, robustness would be considered by including noise factors in the optimization problem [153] and seeking for the solution that is less affected by disruption related noise. Other ways to naturally improve solution robustness is by adding more mission scenarios, to cover more possible cases that the system is expected to be able to anticipate. In short, this particular criterion involves the ability of the method to return a robust solution.

B.3 Applicability

Applicability of method is the last group of criteria for method characterization. Even if correct in theory, not every method is 100% capable of delivering on what is promised for practical problems. Just as the acquisition of a system requires a

minimum number of design cycles to meet the requirements and the objective targets, similarly a method also requires a minimum time period of being validated with several applications, for becoming more effective in practice as well. Other factors that could affect method applicability is the cost of applying the method, either on time or expendable resources, and possible access limitations in tools or data that are pertinent to executing the method. Criteria for method applicability are:

- **Method maturity**. Method maturity refers to the robustness and effectiveness of a method itself. In other words, it is a measure of how well it can deliver a design that will satisfy the prescribed requirements during its entire lifecycle. An incomplete or immature method could potentially result in designs that in practice are not as good they turned out to be on paper. Within method maturity one could include how seamlessly the steps of the method are integrated, as well as the breadth of method applicability.

- **Cost of application**. All methods require some requirements analysis, some modeling and computational analysis and last the investigation of alternative solutions and decision making for the most fit solution. All these steps require plenty of man hours, multiple entities working in parallel and the consumption of resources that may be very expensive to provide. Common issues that address cost of development involve the selected fidelity of the modeling process, prototype testing and validation, as well as plenty of overhead that is allocated on corrections, adjustments and retrofitting.

- **Access and info availability**. Even if all previous criteria are well satisfied, there is still the possibility that stakeholders or involved entities may not have full access to all benefits and functionality of a method, due to regulations, political, social or economical that apply and usually have nothing to with the engineering project itself. For instance, nationality of an associate could

become an obstacle in obtaining full access to a set of data or a model that is proprietary and is of high national security concern. Even if a method is trusted or recognized for its effectiveness, it might still not be as practically beneficial when certain restrictions apply and full access is not authorized.

APPENDIX C

SURVIVABILITY DEFINITIONS IN ENGINEERING DOMAINS

As a complement to the definitions survey on system survivability, this section includes additional discussion for different classes of systems. Excluding military(aerospace, naval) systems, for which survivability has been covered in the main text, the current survey will cover civil transport systems (aerospace, maritime, ground transportation), biological, power and energy systems, as well as communication systems and networks.

C.1 Civil Transportation Systems

Under the category of civil transportation systems, all means of civil or merchant, non-military related, transportation is considered, on land, in sea and in air. Despite the fact that this is a very broad classification involving physically heterogeneous systems, it can be argued that all systems that fall under this class have common mission objectives, operate in similar environments in terms of threats and hazards and are subject to similar human safety requirements and regulations by the associated organizations and administrations. *Air transportation* involves civil transport aircraft, commissioned by airline companies for passenger transport, by parcel and cargo delivery services for cargo and merchant transport and by general aviation companies for private flights. *Sea transportation* includes passenger cruise ships and ferry boats, merchant/tanker ships for cargo transport and private yachts. *Land transportation* is mainly represented by automotive and locomotive systems, utilized either for passenger or cargo transport.

Civil transport aircraft survivability can be defined in the same way as for military systems. Ball's definition [16] is applicable, yet taking into account that the operating environment is less hostile than that of military systems. Emphasis is given towards *safety*, since the most noticeable threats usually involve the operability of the inner system components, mainly affected by reliability, maintenance scheduling and overall dependability. The most severe external threats that a civil transport can experience have to do with terrorist attacks (bombing, sabotaging, highjacking etc.), false or incomplete operational instructions at some point during the mission (machine or human induced, causing collisions, accidents, subsystem damage or fire, etc.) and weather or natural external effects (severe weather, extreme ambient conditions, etc.).

The Federal Aviation Administration (FAA) has developed definitions and procedures for civilian aircraft survivability similar to the safety and combat survivability disciplines. In the context of their Aircraft Hardening Program [81] have formulated an alternative survivability definition. According to FAA [82], survivability is defined as "the absence of a Class I failure after an encounter with the threat", while *FAA Class I failures* include immediate, delayed or landing loss of the vehicle, preventing continued safe flight and landing (Catastrophic failure). FAA safety certification of civilian transport aircraft requires that no Hazard Class I or Class II conditions for single system component failures are acceptable. *Class II failures* (Hazard Level) consists of failure conditions that would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be a large reduction in safety margins or functional capabilities [82], [16]. A civil transport aircraft loss to a hostile threat (kill) is defined as the "inability of the aircraft to continue controlled flight or achieve a survivable landing" [16]. Three loss categories are associated with a Class I Failure: immediate loss, delayed or while airborne loss, and landing loss [16].

Civil transport susceptibility and vulnerability is defined identically to military

aircraft survivability. Susceptibility can be reduced by preventing hazardous devices from being entered onboard, as well as using weapon (SAMs, AAMs, etc.) or electronic detection systems to prevent external attacks. Vulnerability can be reduced by designing the aircraft to withstand the effects of any hit or detonation, either external or internal [16]. Surviving an accident is the result of many factors. Cabin structural integrity, seat belts, seat design, child restraint systems, and brace positions can all increase the likelihood of surviving an impact. Of particular concern is the ability of the cargo area and luggage containers to withstand an internal detonation. Fire retardancy, exit design, aircraft configuration, and evacuation procedures can assist escape efforts after an accident [166].

Despite the differences in operating and threat environments for military and civil aircraft, it has been discussed earlier how some common principles can be applied to assess and improve survivability and safety. The same observation holds for naval surface combatants and passenger cruise ships. For both engineering systems, they have to survive against a threat, attack or damage, yet under quite different constraints, types of threats and environmental conditions. Not unlike to naval ships, the two most common threats for passenger ships are *flooding* and *fire* [173]. Flooding can occur due to ship-to-ship collision or contact, ship grounding. Fire can be initiated by explosion, terrorist act, material failure or human error. Specific to this observation, a definition of survivability for passenger ships has been given by [173] claiming that:

"Survivability is the capability of a passenger ship to continue to carry out its mission in a threat environment that can lead to flood and fire." [173].

Susceptibility, vulnerability and recoverability definitions, while essentially similar to the ones applicable to naval ships, can be adopted for passenger ships, taking into account the peculiar threat and operational environment. While survivability equations can be applied to the assessment process of a passenger ship design, recent efforts have

provided alternative formulations and frameworks for the same purpose. The International Maritime Organization (IMO) back in the early 1960 had organized a series of conventions, known as the *Safety Of Life At Sea* International Conventions (SOLAS), in an attempt to formulate and establish safety and survivability requirements and survivability assessment procedures for passenger and merchant ships [119]. The SOLAS amendments provide regulations on safety and survivability (e.g. regulation A.265 (VIII)), concerning the impact of flooding and fire on ship stability and mobility and furthermore on mission effectiveness and killability. Between damage condition and the total loss/kill of a ship there are many intermediate stages. Based on a naval combatant ship, a hierarchical functional top-down breakdown of the intermediate stages has been outlined by Papanikolaou et al. [173]:

- *Total Kill*, when the ship is either completely lost due to foundering or completely damaged by fire.
- *Mobility Kill*, if loss of ship mobility or controllability occurs.
- *Mission Area Kill*, if a mission related capability is considered lost.
- *Primary or Combat System Kill*, when one or more vital systems of the ship are damaged.
- *Hull, Machinery or Electrical (HM&E) Support System Kill*, if one or more components supporting a primary/combat system of the ship are damaged.

This hierarchical approach essentially implies that a combat/auxiliary system kill can lead to a mission area kill or a mobility kill or furthermore a total kill. Damage extent can also propagate in the opposite direction, for instance, a mobility kill can be reduced to a mission area kill, or to a combat system kill. Equivalently, in a case of a passenger ship, loss of stability due to damage can cause by loss of floatability

(by flooding or foundering), leading to loss of power and ultimately to loss of mobility [173].

C.2 Ground vehicles

Ground transportation systems primarily involve automotive and locomotive systems. Survivability concepts however, in the form that have been earlier defined are effectively represented by safety engineering requirements and enhancement approaches. While one could argue that such systems do not have to encounter threats in a military context, they still experience safety threatening situations and hazards of non-military nature. Combat related threats, such as missile or torpedo attacks, bombing explosions, loss of power could have equivalents for non-combat systems in the form of traffic hazards, natural disasters, sabotaging etc.. It is obvious that combat and ground system threats cannot be compared directly , however, they constitute hazards of similar impact within their own domains.

Susceptibility and vulnerability might not be directly defined for this particular systems type, equivalent measures however exist in the form of *crash avoidance* and *crash worthiness*. Crash Avoidance can be defined as a probability of detecting road hazards and being able to avoid a resulting impact (with external vehicle, body, or obstacle). Kill status for a ground vehicle can occur either after experiencing a direct impact or collision or by catching fire. Crashworthiness is the probability of withstanding an external impact or collision, with the vehicle structure maintaining the minimum required volume and space for the occupants to survive the accident. Subsequently, an equivalent survivability measure could be defined based on the two latter metrics, in similar fashion as with naval and aerospace systems.

Crash avoidance in ground transportation vehicles is implemented through monitoring systems for increased situational awareness along with improved dynamics for enforcing active safety. Future automobiles will feature even more safety systems,

including both active and passive sensors for enhanced threat detection and alerting drivers to impending collision situations [235]. Indeed, the National Highway Transportation Safety Administration (NHTSA) [164], [235] concludes that 70% of rear-end collisions were caused primarily by driver inattention, bringing this threat at the top of the list of hazards on the road. Human-machine interface and ergonomics are also big contributors, in the sense that driver reaction time is critical for understanding the warnings that are provided by the situational awareness systems and complementing the chances of a avoiding impacts or collisions [235].

Crashworthiness on the other hand is closely related to the design and the overall built of the vehicle. Main objective is to preserve a sufficient volume for the occupants to survive the collision without being crushed, or launched outside the vehicle. Structural strength is a key property for maintaining a sufficient survival volume, contributing to a sufficiently strong occupant compartment. Limiting the forces and decelerations the occupants are experiencing to acceptable levels of human tolerance is another significant objective, given that abruptly induced human body motions can be a significant cause of fatality. The resulting effect should be a combination of structural crashworthiness improvements, that would allow portions of the vehicle to crush in a predetermined manner and thus limiting the decelerations of the vehicle. Crash energy management approaches for ground transportation vehicle are very common nowadays for allowing structural crushing to be distributed throughout the entire vehicle, in an attempt to control the behavior of the entire vehicle during the collision [236]. To conclude, this overall collision behavior will determine the vehicle crashworthiness.

C.3 Biological Systems

Survivability in biological systems might have significantly different implications as compared to survivability in engineering systems. According to Darwin's definition,

as provided by his classic text *"On the origin of species"* (1859), survivability is the "evolutionary longevity of species to natural selection" [56]. Alternative definitions describe survivability as the "environmental fitness of organisms" [191]. It appears that survivability in biological species and organisms should require evaluation within large time scales, including complete life cycles or generations.

Organisms have to withstand threats of biological or extinctive nature and typically live inside a changing environment. Thus, susceptibility and vulnerability can still be applicable concepts to complement survivability, given that organisms might employ the same environmental awareness and defense mechanisms. Threats against the long term survival of species can be virus spreadings, pandemic or genocide. Vulnerability is strongly linked to the immunity of organisms to biological threats and in most cases there can be the possibility of recovery, also giving substance to recoverability as third component of the organism's survival.

C.4 Energy Systems

Energy systems is broad category that includes any type of power generation and distribution system, ranging from heavy duty industrial power plants that supply power to cities, manufacturing plants, buildings, to smaller scale systems for supplying power to cars, trains, ships, aircraft and space systems. While size and power output scales form a very large spectrum, fundamentally all types of power system types share something in common: Their basic mission is to be able to convert one form of energy to another (mechanical, electrical, hydraulic, chemical, etc.), thus providing continuous and sufficient power to a network of service loads that serve the mission objectives of the engineering systems that they supply. However, not unlike other engineering systems, they are assigned to deliver these tasks, under the presence of environmental changes and the risk of threats. Thus, survivability in energy systems is critical for the uninterrupted and adequate power delivery. Poroseva has defined

survivability for power systems as [180]

"Ability to provide power to consumers/loads in spite of multiple simultaneous faults caused by natural or hostile disruptions."

Great emphasis is given to the possibility of faults within the system, or power delivery disruptions, given that such incidents can cause a total power outage. Similar factors have contributed towards massive power blackouts, such as the 2003 North-eastern blackout that was discussed in earlier sections. One fundamental difference of a power system as compared to other mobility-driven engineering systems, is that it requires a network of subsystems for power distribution and can thus occupy more space, either in terms of area or volume for accommodating this network. Moreover, it becomes subject to additional threats and hazards that can be common to network or information distribution systems.

Susceptibility and vulnerability are the two main elements of power system survivability, with the former to collect most of the research focus, given the network aspect of the system and the increased demand for more effective situational awareness. to illustrate this point, one should recall that a naval power system is contained within the vessel, occupying space that at worst does not exceed the ship's volume and can benefit from the ship's hardened and shielded external boundaries. On the contrary, an industrial power plant that distributes power to a small town, is not necessarily constrained within the space that the generating unit is occupying. It extends to the entire town through a network of components that can be exposed to several threats and risks. One can understand how the susceptibility of the naval power system is due to its default design lower than for the power generation plant and its distribution system. Thus, to some extent systems are susceptible or vulnerable, based on their default design architecture.

The kill function has a slightly altered implication for an energy system. While

kill for an aircraft is a total system failure (with no recovery option), for a ship "kill" is not always a total ship failure (e.g. foundering) but maybe mission kill, it appears that for a power system "kill" is not a system disaster most of the time but probably failure to deliver power. The dual nature of a power system as an engineering system, but also as a network of distributed subsystems, can interpret a "kill" as a local kill in most cases, that contributes to power delivery irregularities. Unless there are cases of warfare, where an entire power generation and distribution system gets bombed, "kill" cannot destroy the system. As a result, recoverability makes a lot of sense as well, with a heavily supported role in this case for achieving survivable power systems.

Sudhoff (2004) [225] has introduced two additional concepts, *operability* and *dependability*, evaluated with respect to given events. The interface of a power system to systems that consume the generated power consists of *service loads*, which are tasked to perform functions that supports the mission of the end user engineering system (e.g. a propulsion motor, lighting, radar, weapon systems, etc.) [225]. Operability is calculated based on the *operational status* of a load, representing three operational conditions, full, partial or no operation. The input to a load operability can be assigned either by a controller (human operated or automated), or by secondary or side external effects (e.g. high temperature rise in the physical proximity of load that impedes is functionality). Weighting schemes can assign strategic importance ranking to the power system components, defining a relative contribution to system dependability per load. A collective consideration of service load operabilities under a certain weighting scheme (determined usually by mission scenarios) can return a measure for system dependability, thus being an implicit avenue for evaluating system survivability.

C.5 Communications and Networks

Network and communication systems can be classified under engineering systems, however they raise different concerns when it comes to survivability. While they consist of certain engineering subsystems, *system connectivity* and *interdependency* can bring a new understanding in survivability. Systems are not confined in a reserved fixed space, on the contrary there is a spatial distribution of subsystems, adding variability in the threat types a network can encounter based on local environmental conditions. Inner faults or disruptions might pose higher risks for survivability reduction or total mission kill, especially when they can be triggered by natural or emergent disturbances.

From a network theory perspective [6], survivability in a communications channel is defined as the:

"probability of retaining connection between representative pairs of nodes." Survivability

is framed around system connectivity in this version, hinting that disrupted connections may be the most common threats against the propagation of energy or information through a network. The Federal Communications Standard 1037C brings a detailed definition [233]

"Survivability is a property of a system, subsystem, equipment, process, or procedure that provides a defined degree of assurance that the named entity will continue to function during and after a natural or man-made disturbance."

While the essence of the definition is not nay different than earlier ones, there is an indication that natural disturbances play more significant roles in affecting networked system operations. Baran may have the most inclusive definition, including the aspect of physical attacks, the multitude of engineering systems connected through a network and the importance of maintaining connectivity:

"Survivability is the percentage of stations both surviving the physical attack and remaining in electrical connection with the largest single group of surviving stations." Shifting towards an information technology systems network perspective, Deutsch [61] defined survivability as *"the degree to which essential functions are still available even though some part of the system is down"*, giving emphasis in *function value delivery*, possibly due to the fact that the main objective of a computing system is to deliver an outcome through a returned value. The kill mode in this case would not be a totally destroyed system, nor its operator or controller, but failure to deliver a value. Ellison et. al provided another suitable definition [72]:

"Survivability is the ability of a network computing system to provide essential services in the presence of attacks and failures, and recover full services in a timely manner."

essentially shedding more light on the issue of "function/service value delivery", the types of attacks possibly encountered and bringing in the aspect of time constrained recoverability. Recoverability might be desired for assuring that the system will keep functioning and delivering, however at some point the quality of service will be questioned by stakeholders or service recipients, therefore bringing the system closer to its original performance condition is the ultimate requirement for a survivable and resilient system.

Ellison et al. [72] extended their definition by describing survivable systems through providing specification for survivable systems. This includes:

1. A precise description of the operating environment
2. The functions that the system must provide.
3. A preferred order of provision of the functions.

4. Probability distributions to describe the uncertainty regarding the system's operating conditions, function and function prioritization.

Knight et al. [134] has adopted a similar specification approach to defining survivability and extended it to include customer values and expectation and repackaged all information in a state vector, also known as the *survivability specification vector*:

$$S = [E, R, P, M] \tag{87}$$

where S is the survivability specification state vector, E represents the assumed operating environment, R describes the services that the system must provide, P is a probability distribution across the set of specifications R. and M is a system representation [S, s_0, V, T] with s_0 as the initial or preferred state for the machine, V is finite set of customer values and T a state transition matrix.

Network systems do include survivability associated metrics that are equivalent to susceptibility and vulnerability. The kill state in this domain is referred to as *fault*. As Knight (2000) remarks, "the informal notion of an event that causes damage which we have used is referred to formally as a fault" [134]. *Fault tolerance* is the systems property to withstand and survive the effects of the fault, namely representing the same concept as system vulnerability for engineering systems. *Fault avoidance* similarly links to susceptibility, in terms of how prepared or equipped the system is to avoid the fault.

As explained in Chapter 1, survivability is a dependability property for networks. Survivability according to Knight "is not synonymous with fault tolerance". Fault tolerance is a mechanism that can be used to achieve certain dependability properties. If one imagines fault tolerance as resilience, a similar association holds with regard to survivability. Resilience is philosophy that can be enabled by survivability and deliver more dependable systems. With increased dependability, "a system can be considered reliable, available, secure, safe, survivable etc." [134]. Describing a system as fault

tolerant is really a statement about the system's design, not its dependability. To complete this survey, the concepts of *fault elimination* and *fault forecasting* directly match to recoverability and situational awareness. As Knight [134] adds, improvement in all four enabling mechanisms/properties can significantly improve systems dependability through survivability.

APPENDIX D

THE GOAL-QUESTION-METRIC METHOD

Development of metrics has been a key exercise for the resilience assessment framework. Given that resilience engineering is an emerging discipline, with few quantitative formulations available from current literature, a clean sheet approach has been necessary. Metrics are necessary enablers for the practice of engineering discipline, and a tool for evaluating performance in engineering. The development of the appropriate metrics must be anticipated as a disciplined science itself, rather than an Ad Hoc exercise. Therefore, a number of metric development approaches were discovered and evaluated. The choice of method for this crucial methodological step, was the G-Q-M, or Goal-Question-Metric technique, suggested by the INCOSE [261].

According to the G-Q-M guide, a metric is a standard of measurement. A typical lifecycle for a metric is formed by the following steps:

1. Define measurement goals.
2. Collect and validate metric data.
3. Analyze metric data.
4. Derive metric knowledge.
5. Improve product process operating procedures and decision making.

There are four main categories under which every metric can be classified. According to its mathematical description, a metric can be at least one of the following:

- Ratio: Division of one quantity over the other, with the numerator and denominator being mutually exclusive.

- Proportion: Division of one quantity over another, with the numerator and denominator not being mutually exclusive and the numerator is part of the denominator.

- Percentage: A conversion of a proportion in terms of -per hundred- units.

- Rate: A rate represents the dynamic rate of change of the phenomena of interest over time.

A good metric must be characterized by accuracy, precision, validity and correctness. Accuracy is the degree of agreement of individual or average measurements with an accepted reference value or level, while precision is the degree of mutual agreement among individual measurements made under prescribed conditions, or simply how well identically performed measurements agree with each other. Validity is the degree at which the metric really measures what it is intended to measure, for instance the extent to which an empirical metric reflects the real concept under consideration. Last, correctness infers that the data was collected according to the exact rules defined in the metric, e.g. conditions at which data were collected for metric evaluation.

As an illustrative example, it is assumed that a goal imposed by a stakeholder is to "increase product reliability". As a consequence, a relevant question can be formulated as follows: "What is the current fault removal rate compared to earlier releases of this product"? One metric that answers to the previous question is the current percent and number of faults removed by lifecycle phase and fault severity for this product release. Another possible metric is the previous percent and number of faults removed by lifecycle phase and fault severity for earlier releases.

Linking this simple example to the resilience framework and to system capability, there can be at least two metrics of interest derived. Following the G-Q-M approach, the two goals for the system are:

- G1: Improve ability to minimize capability loss.

- G2: Improve ability to meet critical thresholds.

Two questions can be formulated as an attempt to explore possible metrics for the measuring of the system's ability to satisfy the two previous goals:

- G1-Q1.1: What is the capability loss due to performance degradation?
- G1-Q1.2: What is a time dependent average measure of the capability loss due to performance degradation?
- G2-Q2: To what extent is the threshold satisfied, even after significant performance degradation?

At this point, metrics can be formulated as possible answers to the goals and questions:

- G1-Q1.1-M1.1: The capability loss due to performance degradation can be expressed as:

$$MC_L = MC_0 - \bar{MC}_T \tag{88}$$

- G1-Q1.2-M1.2: The time weighted average capability can provide a cumulative time-dependent measure of the system's response due to performance degradation:

$$\bar{MC}_T = \int_{t_0}^{t_0+\tau} (MC_0 - MC(t))dt \tag{89}$$

  with as the time-averaged capability loss

- G2-Q2-M2: Threshold availability A_T, where, TAT is the total Time Above Threshold:

$$A_T = TAT/T \tag{90}$$

APPENDIX E

CHARACTERIZATION OF A THREAT ENVIRONMENT

A military system that has to operate under several external threats, safety risks and other types of disturbances. In order to explore the options for improving the effectiveness of a military system by design, a complete understanding and investigation of the threat environment is critical. Figure 190 contains some of the basic criteria for describing a threat.

E.1 Origin and direction

The threat characterization criteria have been conceived by thinking of a threat as a physical entity that can change the value of some of the properties of its surrounding environment[109]. Space time are the first properties of a threat that can come in mind. A threat starts from a certain location and propagates towards one or multiple other locations. Thus, a threat can be described by its *origin* and its *direction*, not unlike a vector in 3-dimensional space. The threat may then propagate towards a single or multiple direction. In the single direction case, the threat can be viewed as a vector. For instance, a Surface-to-Air (SAM) missile system, will launch a missile on a single path that follows the adversary single target. In the multiple direction case, the threat propagates in two or infinite number of directions, effectively creating a field where mass, momentum and energy is propagated. A bomb explosion, a disease transmitted through a virus or a force field are examples for multi-spread threats.

E.2 Environmental morphology

A significant factor on how a threat will be deployed, is the *morphology* of the environment that the threat will propagate. In an analogy to the propagation of an

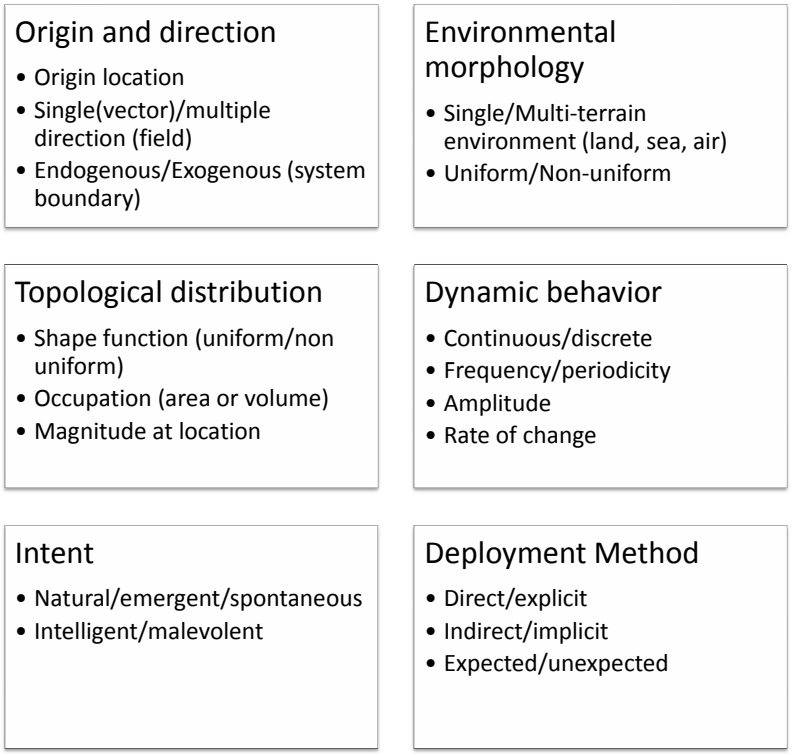


Figure 190: Criteria for threat characterization

electromagnetic wave, this would correspond to the mean that the wave travels in. Aside from the standard forms of matter, namely solids, liquids or gases, at a higher level the distinction will include land, sea or air. The threat environment may also involve multiple terrains. A good example of the latter is a land-air based theater of operations [16]. A *Surface-to-Air* gun system or missile launcher (SAMs) can be a land or sea based threat for adversary aircraft. Other alternatives are *Air-to-Air* gun systems or missile launchers. or *Air-to-Surface* aircraft installed gun systems or missile launcher for targeting land or sea based strategic fixed or mobile targets. Last, another feature of the threat environment is the uniformity of the terrain. Land can be flat (uniform) or bumpy (non-uniform). Similarly, liquids or gases may have constant or varying density. The frequency of transitions from one terrain to another is another factor that makes the environment highly non-uniform.

E.3 Topological distribution

Returning to the threat propagation itself, another criterion is the environmental space that it occupies. To better illustrate this feature, an analogy is drawn from structural dynamics. As part of a larger structure, a beam column is designed to support a maximum amount of load, and in many cases the load distribution shape is constrained. There can be an unlimited range of load distribution shapes, yet uniform, triangular (linear) or quadratic (nonlinear) are the most common ones. Highly non-linear and dynamic load distributions require more sophisticated computational techniques (e.g finite element methods) to determine the design of the beam. If the load distribution on a beam can be visualized as a "threat" that will cause the beam to translate, rotate or bend, then a threat can be topologically described as a load distribution. In other words, a threat is characterized by a shape function, implemented as a normalized mathematical functions of space $f(x, y, z)$. At each point (x,y,z) a *magnitude* $m(x, y, z)$ that describes the possible impact of the threat on that location. The bounded area or volume that any possible threat impact is defined within, defines the total *occupation* of the threat.

E.4 Dynamic Behavior

A threat is characterized by its dynamic behavior. Except for the cases where a threat is manifested by an *impulse*, namely an act of a finite amplitude in a infinitesimally small time, in most cases a threat propagates for certain time period with a finite *duration*. If the threat is conceptualized as a time-varying signal, it can either be a *continuous* or *discrete* signal. A disease that geographically spreads with an increasing impact intensity is described by a continuous signal that varies in space (x, y, z) and time t. On the other hand, a series of bombing attacks that occur at different time instances and possibly at different locations are described by a discrete signal, representing a chain of discrete events. In either case, both signal types are

characterized by their *amplitude* $A(t)$, namely the magnitude of the disturbance as it varies with time. The *periodicity* of the signal indicates how often discrete events occur, or when the continuous signal reaches its maxima, or minima. For a pure periodic behavior, the *frequency* of the signal ω is defined for either signal type. For continuous signals, a *rate of change* for the amplitude is defined, and along the same lines, a *gradient* vector is defined for the spatial propagation of the threat

E.5 Threat deployment:Intent and propagation methods

In a less quantitative characterization criterion, threats are assessed from a strategic and causal perspective. A threat occurs due to the objectives or intents of a certain party that seeks to accomplish a particular goal. A nation's military force in a battlefield, a terrorist group's unexpected action against a country, or the disease that spreads itself to survive are all examples of entities that spread a threat, in order to achieve a goal. Thus, every threat contains an *intent*, that typically depends on the nature of the end goal. Threats can be *natural* and furthermore, *spontaneous* or *emergent*. A natural threat implies that there is no human interference that contributes to its manifestation. Natural effects due to weather or climate change are good examples of natural threats. Hurricane Katrina [132] is a recent example of a natural event that spontaneously occurred and became a threat to the entire infrastructure of the city of New Orleans, and eventually triggered a large scale disaster. On the other hand, the 2003 Northeastern Blackout is another example of a natural threat that was initiated by a small scale fault (spontaneous threat), but the inherent interdependencies of the power distribution system allowed for a series of emergent events that resulted in a another large-scale disaster.

Non-natural threats are usually *intelligent* human-induced threats that end up being *malevolent* for the systems or groups that they target. Force projection against the enemy in the battlefield is an intelligent threat. To elaborate further, there can

be many different styles or methods on how the force projection is executed. The *deployment method* is a contributing factor on intense this threat is going to be for the enemy target. For instance, the Navy doctrine on warfare, dictates two basic styles of naval warfare at sea, *attrition* and *maneuvering* [163]. With attrition, the objective is to wear down the enemy in a direct one-to-one type of conflict. While attrition is a direct method of force projection, maneuvering is an indirect warfighting style that employs a higher pace of tactics and responses towards the enemy is adopted.

Military related threats are usually *expected* threats. *Terrorism* is another form of intelligent threat with malevolent intentions. A great variety of weapons are used, from bombing equipment, to chemical or biological weapons [23]. As part of their method of deployment, acts of terrorism are *unexpected* in terms of their location and timing of occurrence. Targets of terrorism are beyond military systems, it appears that civilian transportation, power generation or communications systems are also common strategic targets that terrorists prefer. Where military systems are designed with their greater exposure to threats in mind, civilian targets are not designed with reduced susceptibility and vulnerability requirements as a first priority. To illustrate this point, one can consider two historic terrorist attacks, such as the U.S.S. Cole [90] bombing and the Pan Am flight 103 Boeing 747 Jumbo jet bombing [172]. While they both suffered a similar initial blast as the primary effect, the civilian system experienced a total catastrophic failure, while the military system managed to protect itself from catastrophe by not allowing the blast damage to propagate throughout the rest the system.

In a more systematic investigation of threat impact, threats can be tabulated against system types, resulting to a threat-system matrix classification. This is a useful approach to distinguish the most dangerous types of threats that need to be avoided and can be instrumental for visualizing the threat overlaps across different types of systems. Table 8 contains a set of basic system types against possible threats

that they can encounter, classified according to their individual characteristics.

Table 8: Threat classification for various system types

	Types	**Intelligent**	**Natural**
Military	Fighter a/c	Enemy threat	Heavy weather
and	Rotorcraft	Terrorism	Workplace hazards
Defense Systems	Naval ships	Chemical/Bio	Grounding
	UAV		Collisions
Civil	Passenger aircraft	Terrorism	Heavy weather
Transportation	Passenger ships (Ferries)	Chemical/Bio	Workplace hazards
Systems	Merchant ships	Attack	Operational errors
	Ground transportation	Hijacking	Collisions
Energy	Power distribution	Enemy threat	Capacity overload
Systems	Intelligent power grids	Terrorism	Component damage
	Nuclear plants	Chemical/Bio	Extreme weather
Networks and	Communications	Terrorism	Capacity overload
Communications	IT support networks	Hijacking	Component damage

The purpose of including a thorough threat analysis in the present section aims at making the case that a system design may not be effective in a real life application or mission, if the possible threats expected to be encountered are not going to be taken into account during the design process. In theory, a system design may contain the capability to perform as expected, but its design must imply that it contains the additional capacity of absorbing the effects of a threat, either through safety margins, system survivability and robustness. A threat analysis supports a threat assessment procedure that is necessary to collect information on the impact that a threat may have on a particular system design. It can further help reveal other subsequent modes of failure after the initial damage (e.g bombing blast). Damage propagation and resulting effects (e.g. catastrophic failure or disaster) are dependent on how vulnerable systems are or if and how they could recover from this situation. With this information, system designers car investigate possible remedy actions towards increasing vulnerability and recoverability. However, it appears that only until recently, there have been efforts aiming to address vulnerability design issues as part of the early

conceptual design process. While such efforts have mainly been initiated by the military systems design community, the benefits can become obvious for civil applications as well.

It is one of the objectives of this research to establish the need for addressing the same mission uncertainty and risk concerns for any other type of engineering system, e.g. civil transport aircraft, passenger/merchant ships, ground transportation system, power generation and distribution network infrastructures, etc. one of the visions, pertinent to this work is that all systems can be expected to operate under threats against their mission. While understanding that threat uncertainty and risk is not the same for all systems, there must still be an initiative for improving the design for improving the inherent ability of withstanding the resulting effects of a threat and protecting the system's physical integrity and human operators.

APPENDIX F

CANONICAL PROBLEM: DESCRIPTION AND MODELING APPROACH

In order to demonstrate the applicability of the proposed metrics, a small scale canonical problem has been constructed. The purpose of the particular pilot problem is to be a flexible and easy to understand platform, where the basic steps for the resilience assessment analysis, and the effectiveness of the metrics can be demonstrated. The model for the canonical problem has been constructed in a way that it carries the minimum required behavioral characteristics of a larger scale complex system. At the same time, the system configuration must scalable and modular, so that the model can be easily revised and adjusted to the problem requirements, e.g. for performing uncertainty analysis, control design, etc. Last, it must be an efficient implementation that allows for rapid parametric analysis and exploration.

F.1 Introduction

A spring-mass-damper system (SMD) with a multi-spring configuration has been selected and implemented as the canonical model for method development. At the baseline configuration, the SMD system consists of a mass m that can move along the x direction, essentially being a single degree of freedom system (SDOF). The mass is bounded on both sides, by two walls, which are at a distance of x_{ult} from the equilibrium point $x_0 = 0$.

The experimental setup also includes a damper of damping ratio ζ and an array of 8 main springs. The springs are equally distributed in either side of the mass, having 4 springs at each side. The springs are characterized by their stiffness k_{0i}, where $i =$

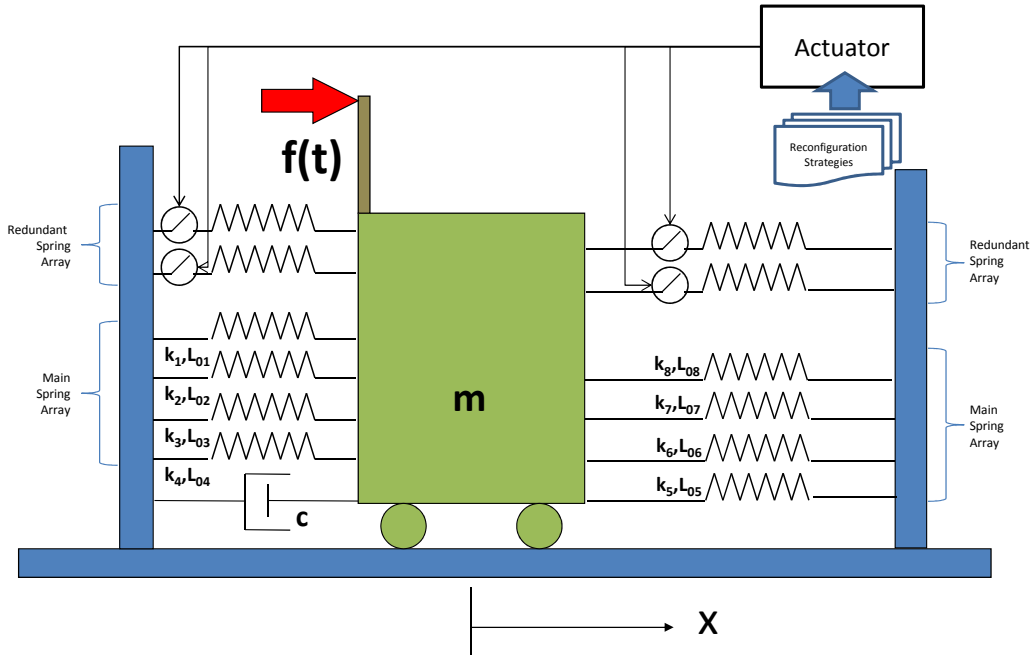


Figure 191: Canonical problem configuration

1..8, while this stiffness is the initial stiffness that spring has by design. Also, springs are allowed to degrade at an exponential rate λ_i, when the force F_{spring_i} on a spring i reaches a critical threshold F_{crit_i}. In other words, the variation of the stiffness for spring i is expressed as:

$$k_i = \begin{cases} k_{0i} & \text{if } F_{spring} < F_{crit_i} \\ k_{0i} \cdot exp(-\lambda_i \cdot t) & \text{if } F_{crit_i} \leq F_{spring} \leq F_{ult_i} \\ 0 & \text{if } F_{spring} > F_{ult_i} \end{cases} \tag{91}$$

The system is losing its stiffness, when it breaks after reaching the ultimate force threshold F_{ult}. Stiffness information is a given input to the system in the form of a user defined input file. Similarly, stiffness critical values can be passed on the system, which depend on the material the springs are assumed to be made of. A schematic of how the SMD system is configured, is given with Figure 191.

The basic mission of the system is to vibrate around its equilibrium point, but ensure that it will not get out of the designated bounds. For its normal operating

conditions, a nominal constant force $p = p_0$ is applied on the mass, in order to maintain a stable oscillation. However a second external, time-dependent load distribution applies on the mass unexpectedly, thus adding more energy on the system. In some cases, the system may be able to compensate the impact of the additional force by itself. In some other cases through, it fails to completely neutralize these effects, thus experiencing increasing displacements and accelerations, and eventually become destabilized.

As part of its mission, the system must be capable of withstanding an instantaneous impulse or loading $d(x,t)$ that is dynamically acting over a certain period of time τ. A general form of the disturbance input is:

$$d(x,t) = d_0 * f_{1d}(x) * f_{2d}(t) \tag{92}$$

assuming that spatial and temporal contribution can be independent. The magnitude d_0 is expressed as a force (kN). The factors $f_{1d}(x)$ and $f_{2d}(t)$ are normalized functions that describe the disturbance spatial distribution on the layout and the amplitude respectively. For the particular experiment, the spatial distribution is uniform, implying that the load can act at ny location. The temporal part however, is selected by the user, and can either be a step function, or sine signal input. There is no limitation on the input signals, but the latter two are the ones considered for the current experiment.

Along these lines, the system must remain within bounds, while in terms of its integrity, it must take the appropriate actions, in order to protect as many springs as it can, preventing them from reaching the breaking limit. In other words, system health is determined by the collective "health" status of all the main springs. Moreover, it is also expected to recover from temporary effects that unexpected time-dependent disturbance loading has induced, maintaining as much of its structural health as possible. This implies that a certain level of damage control is required. a rule based, feedback controller is included for this layout, which is responsible for

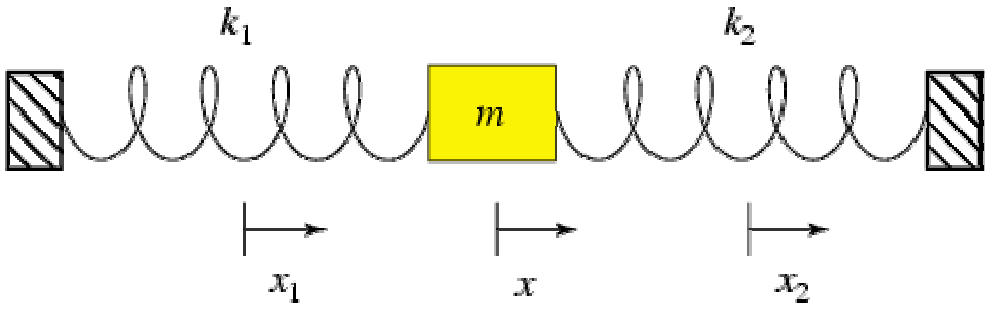


Figure 192: Simple two-parallel spring configuration

sensing the stiffness of each spring, and furthermore manage total system stiffness, by enabling/disabling main or a range of redundant springs accordingly. An array of four additional springs is included, which can be selectively enabled through an actuator, that is controlled by the rule-based controller.

F.2 Modeling approach

For implementing the model, some basic ideas must be clarified as part of the modeling approach. The springs are configured in parallel, in groups of four. Figure 192 contains a simple example, with two springs that are connected to a mass in parallel. The other end for each spring is attached on a fixed wall, while k_1 and k_2 are the spring constants. A displacement of the mass by a distance x results in the first spring lengthening by a distance x_1, while the second spring is compressed by a distance x_2.

Starting from force balancing for the diagram of Figure 192, the governing equation for the system is given by Equation 93

$$m\ddot{x} = -k_1 x - k_2 x = -(k_1 + k_2)x \tag{93}$$

which returns:

$$\ddot{x} = -((k_1 + k_2)/m)x \tag{94}$$

The effective total stiffness of the system is:

$$k_{eff} = (k_1 + k_2) \tag{95}$$

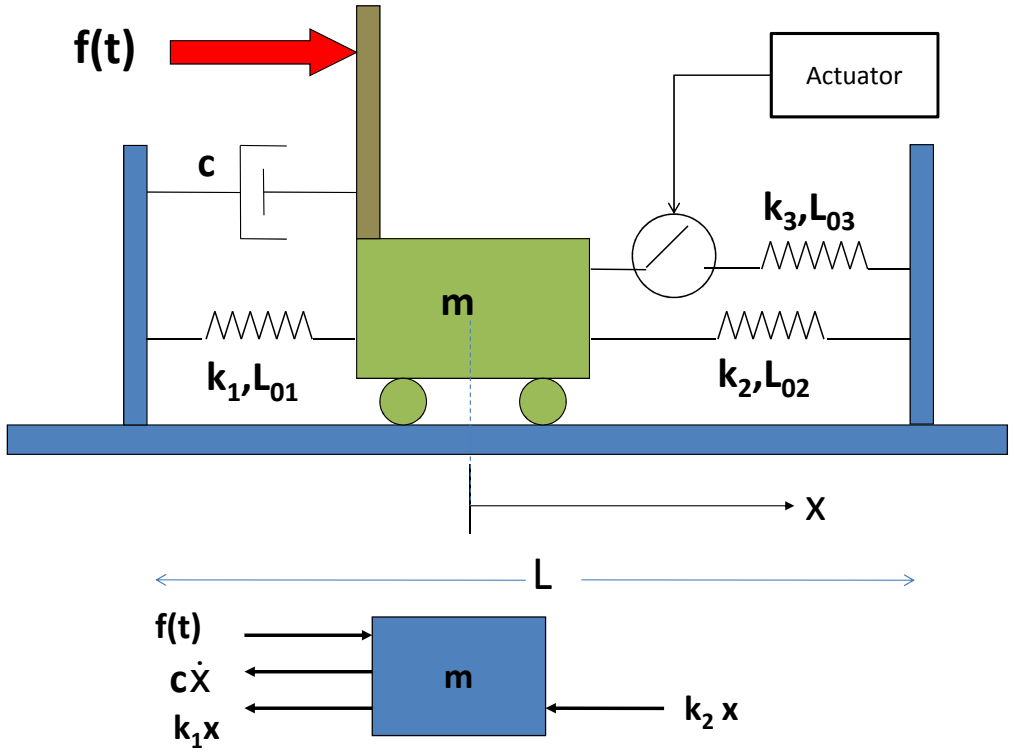


Figure 193: Simple two-parallel SMD configuration

while the natural frequency is calculated as:

$$\omega = sqrt((k_1 + k_2)/m) \tag{96}$$

Figure 193 expands on the previous simple parallel spring model, to include the damper, along with a redundant spring for recoverability. Following the same approach and starting from the free body diagram, the governing equation is:

$$m\ddot{x} = f(t) - k_1 x - k_2 x - c\dot{x} \tag{97}$$

assuming an input force $f(t)$, and $x_0 = 0$. The total stiffness is identical to that of Equation 95, as well as the natural frequency being identical to Equation 96.

F.3 MATLAB/Simulink implementation

The computational model for reconfigurable multi-spring SMD model has been implemented in MATLAB/Simulink. While earlier sections offered a short introduction

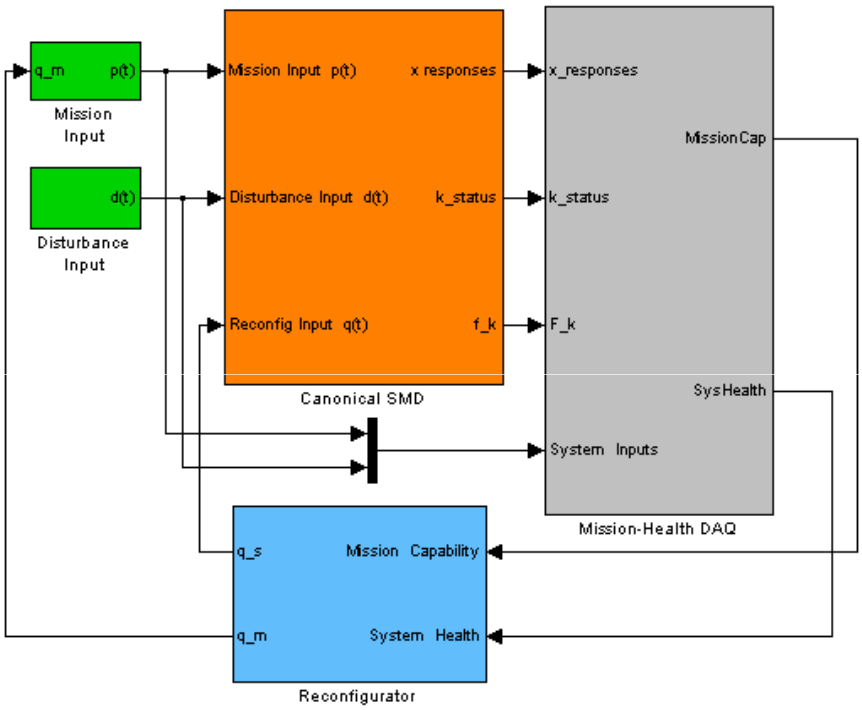


Figure 194: Computational model implementation layout

to the basics of the modeling approach, this section will elaborate on the features of this particular architecture, as the key layers of the model are discussed. Figure 194 offers an overview of the simulation model topology. It includes the input modules, through which one can select the magnitudes and signal shapes for the mission and disturbance inputs, the main SMD simulation, the blocks with the spring arrays, properly connected to the system, along with the damper. Last, the rule based controller is another significant component, for allowing the system to reconfigure itself and restore its mission responses, while the last model is an inclusive data collection and processing module, for storing the experimental data outputs.

The core of the simulation is the second order solver, which returns the solutions for the displacement $x(t)$, the velocity $\dot{x}$, and the acceleration $\ddot{x}$. An overview of the implementation is shown in Figure 195. The spring plant contains the topology implementation for the springs, while the total stiffness is aggregated for forming the

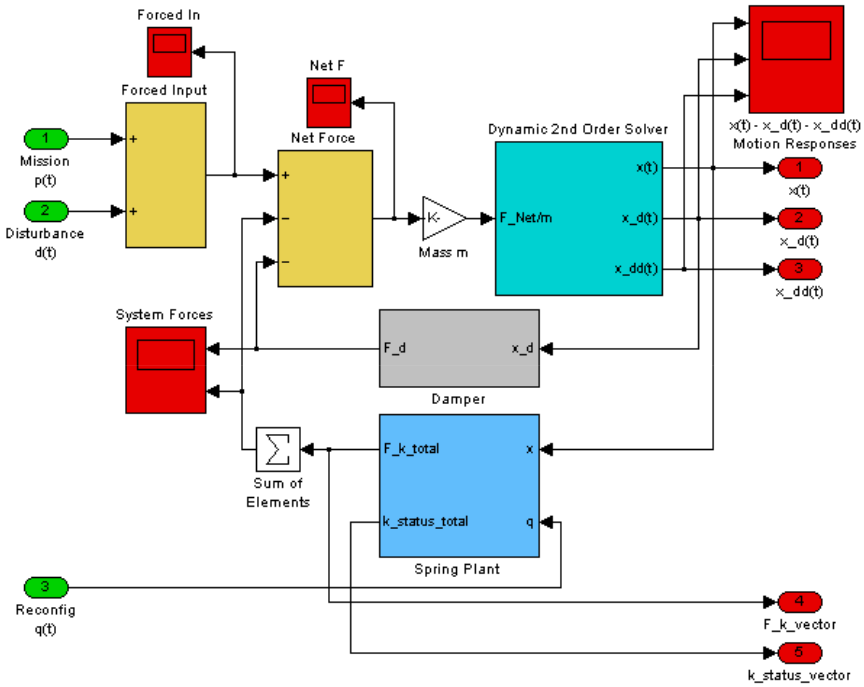


Figure 195: Second order SMD solver

corresponding terms of the governing equation. The same plant also provides real time information on the status of each spring based on its actual contribution. This information is collected by the information acquisition, as well as by the controller.

The spring plant consists of two smaller plants of parallel connected springs in groups of 4, along with a third block that contains two smaller blocks of two backup springs each. The model allows for a user input on the spring's status, a feature that allows for experiments where the spring could randomly break, regardless of its nominal health status and operating conditions. The output of this block is the total spring force, along with the vector that contains the time histories of the spring health status. Figure 196 provides a view of the spring block.

The reconfiguration block is the part of the simulation that contains the rule based controller, along with the actuator. The role of the controller, is to collect the status of the springs in real time, along with system capability information (e.g. how well it satisfying its operational constraints). From a practical standpoint, the controller is

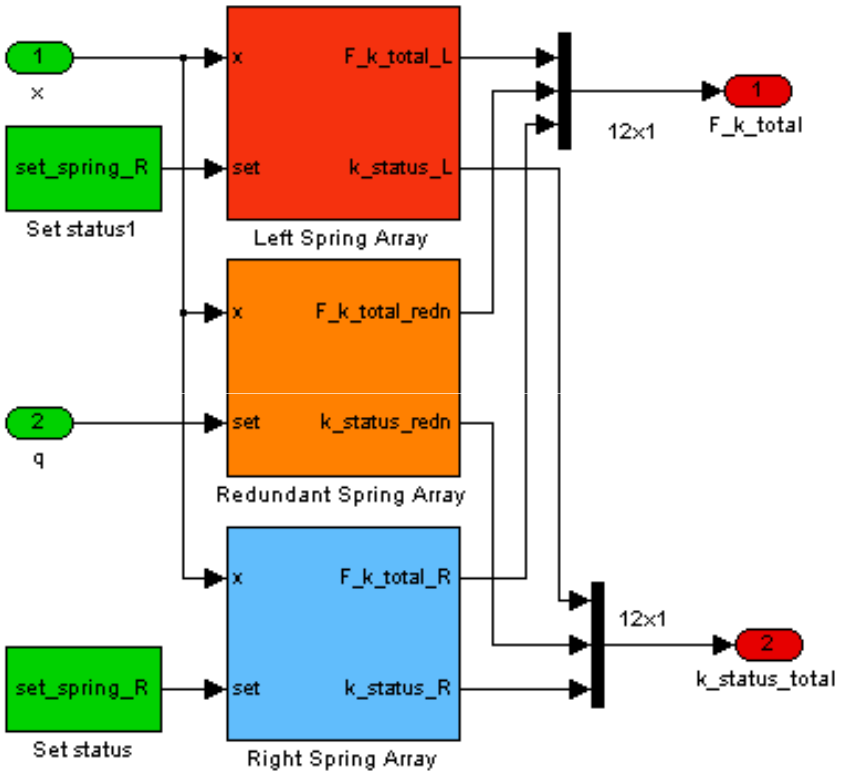


Figure 196: Spring plant block

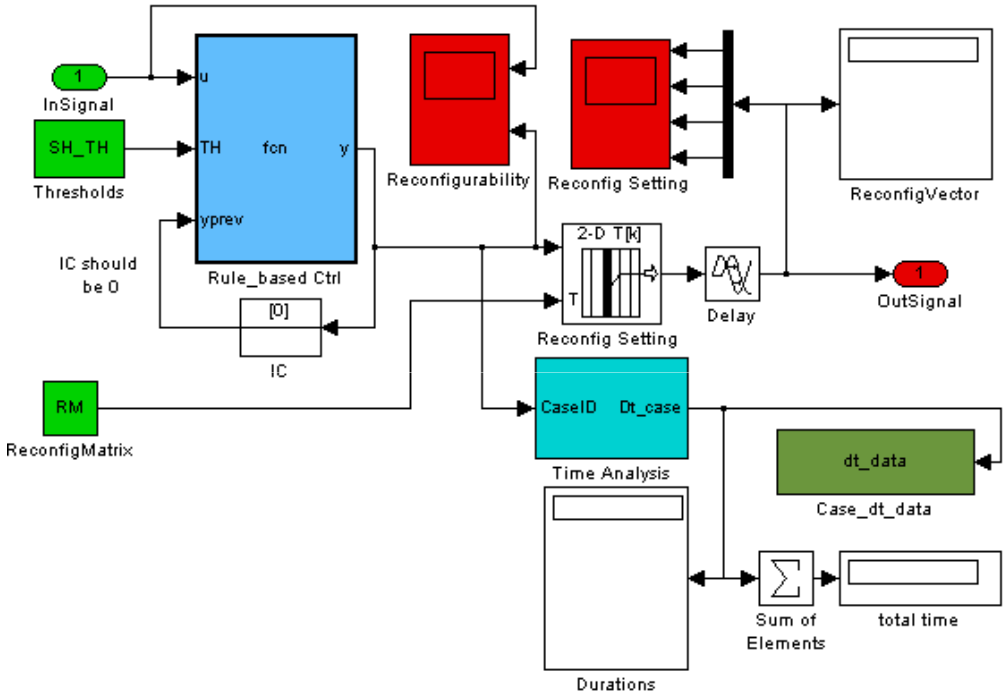


Figure 197: Reconfigurator block

comparing system capability real time data to the critical thresholds. Based on the system's position, namely, the zone of thresholds that its value lies between, it selects the appropriate reconfiguration strategy that corresponds to the zone, and returns a signal with spring operating commands, which is propagated to the spring plant.

The last block is the information collection block. It is the block responsible for processing the simulation response $x(t)$, in order to obtain $MC(t)$ time histories, as well as for converting spring stiffness data to a measure for total system health $SH(t)$.

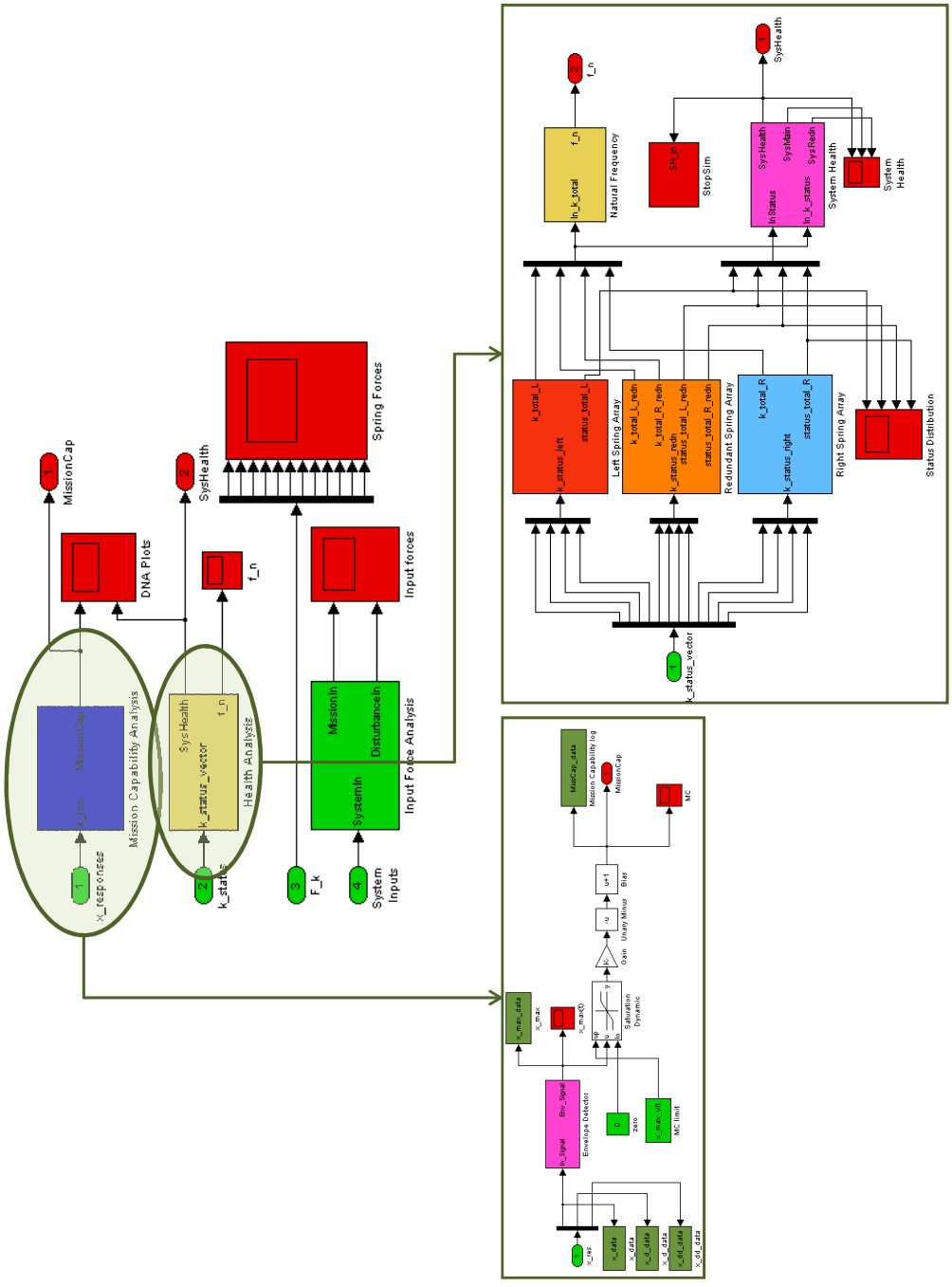


Figure 198: Information collection block

REFERENCES

[1] "The next revolution at sea," August 2003.

[2] "Annual review: Natural catastrophes 2004," 2005.

[3] Ackoff, R. L., "Towards a system of systems concept," *Management Science*, vol. 17, pp. 661–671, July 1971.

[4] Adger, W., "Social and ecological resilience: are they related?," *Progress in Human Geography*, vol. 24, no. 3, p. 347, 2000.

[5] Aerospace Systems Design Laboratory (ASDL), "Integrated Reconfigurable Intelligent Systems (IRIS).," May 2003.

[6] Al-Noman, A., "Analysis and evaluation of survivability of various configured communication networks," *International Journal of Communication Systems*, vol. 11, no. 5, pp. 305–310, 1998.

[7] Alhazbi, S., "Measuring the complexity of component-based system architecture," in *Information and Communication Technologies: From Theory to Applications, 2004. Proceedings. 2004 International Conference on*, pp. 593–594, IEEE, 2004.

[8] Alion Technologies, "Measure of Total Integrated System Survivability (MOTISS)." Online, May 2009.

[9] Allenby, B. and Fink, J., "Toward inherently secure and resilient societies," *Science*, vol. 309, no. 5737, p. 1034, 2005.

[10] Amaral, L. and Ottino, J., "Complex networks: Augmenting the framework for the study of complex systems," *The European Physical Journal B-Condensed Matter*, vol. 38, no. 2, pp. 147–162, 2004.

[11] Anderson, P., "Complexity theory and organization science," *Organization Science*, vol. 10, pp. 216–232, May-June 1999.

[12] Apostolakis, G., "How useful is quantitative risk assessment?," *Risk Analysis*, vol. 24, no. 3, pp. 515–520, 2004.

[13] Attoh-Okine, N., Cooper, A., and Mensah, S., "Formulation of resilience index of urban infrastructure using belief functions," *Systems Journal, IEEE*, vol. 3, no. 2, pp. 147–153, 2009.

[14] Aviation Week, "The space shuttle's lessons for the future." Online, December 7 2010.

[15] Avizienis, A., Laprie, J., and Randell, B., "Fundamental concepts of dependability," tech. rep., University of Newcastle upon Tyne., Computing Science, 2001.

[16] Ball, R. E., *The Fundamentals of Aircraft Combat Survivability Analysis and Design*. American Institute of Aeronautics & Astronautics (AIAA), 2003.

[17] Ball, R. E., "Design for survavibility," *Aerospace America*, vol. 11, pp. 32–36, 2005.

[18] Ball, R. E. and Atkinson, D. B., "A history of the survivability design of military aircraft," tech. rep., AIAA, 1998.

[19] Bantre, M., "Deliverable D13: From resilience-building to resilience-scaling technologies: Directions," tech. rep., ReSIST: Resilience for Survivability in IST, 2006.

[20] Bar-Yam, Y., *Dynamics of Complex Systems*. Perseus Books, 1997.

[21] Barber, D., *Weapon System Effectiveness Industry Advisory Committee (WSEIAC) Final Report of Task Group II: Prediction Measurement*. Defense Documentation Center, 1965.

[22] Bascunana, J., "Analysis of lane change crash avoidance," tech. rep., Society of Automotive Engineers, 400 Commonwealth Dr, Warrendale, PA, 15096, USA,, 1995.

[23] BBC World Online, "Biological and chemical warfare - modern day threat." Online, January 2009.

[24] Biltgen, P., *A Methodology for Capability-Based Technology Evaluation for Systems-of-Systems*. PhD thesis, School of Aerospace Engineering, Georgia Institute of Technology, 2007.

[25] Bogard, W., *The Bhopal Tragedy: Language, Logic, and Politics in the Production of a Hazard*. Westview Press, 1989.

[26] Boulougouris, E. K. and Papanikolaou, A. D., "Optimisation of the survivability of naval ships by genetic algorithms," in *3rd Int. EuroConference on Computer Applications and Information Technologies in the Maritime Industries*, May 2004.

[27] Boulougouris, E. K., Papanikolaou, A. D., and Zaraphonitis, G., "Optimization of arrangements of Ro-Ro passenger ships with genetic algorithms," tech. rep., National Technical University of Athens, Ship Design Laboratory, Athens, Greece, 2003.

[28] Bowman, A., "An integrated electric power system: The next step." Online, 2004.

[29] Boyd, J., *Strength of materials*. McGraw-Hill, 1917.

[30] Brown, A. and Chen, D., "Probabilistic method for predicting ship collision damage," *Ocean engineering international*, vol. Volume 6, No. 1, pp. pp. 54–65, 2002.

[31] Brown, A. and Mierzwicki, T., "Risk metric for multi-objective design of naval ships," *Naval engineers journal*, vol. 116, no. 2, pp. 55–72, 2004.

[32] Brown, A. and Salcedo, J., "Multiple-objective optimization in naval ship design," *Naval Engineers Journal*, vol. 115, no. 4, pp. 49–62, 2003.

[33] Brown, A. and Thomas, M., "Reengineering the naval ship concept design process," in *From Research to Reality in Ship Systems Engineering Symposium, ASNE*, September 1998.

[34] Browne, R., "C4I defensive infrastructure for survivability against multi-mode attacks," in *MILCOM 2000. 21st Century Military Communications Conference Proceedings*, vol. 1, pp. 417–424, IEEE, 2002.

[35] Bruneau, M., Chang, S., Eguchi, R., Lee, G., ORourke, T., Reinhorn, A., Shinozuka, M., Tierney, K., Wallace, W., and von Winterfeldt, D., "A framework to quantitatively assess and enhance the seismic resilience of communities," *Earthquake Spectra*, vol. 19, p. 733, 2003.

[36] Bush, G., "Homeland Security Presidential Directive-3." online, March 11 2002.

[37] Caralli, R., "Sustaining operational resiliency: A process improvement approach to security management," tech. rep., NASA Center for AeroSpace Information, 2006.

[38] Carlson, J. and Doyle, J., "Complexity and robustness," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 99, no. Suppl 1, p. 2538, 2002.

[39] Castet, J. and Saleh, J., "Survivability and resiliency of spacecraft and space-based networks: a framework for characterization and analysis," in *AIAA SPACE 2008 Conference*, American Institute of Aeronautics and Astronautics, 1801 Alexander Bell Drive, Suite 500, Reston, VA, 20191-4344, USA,, 2008.

[40] Chief of Naval Operations, "Navy system safety program policy," 2007.

[41] Christensen, W. and FE, C., *Safety Through Design*. National Safety Council, 1999.

[42] Civil Aviation Authority (CAA), "Aircraft hardening research program: Final overview report," tech. rep., Civil Aviation Authority (CAA), London, 2001.

[43] Clayton, D., Jebsen, G., and Sofia, J., "The All Electric Warship from vision to Total Ship System Integration," tech. rep., Naval Sea Systems Command, Office of Naval Research Naval Surface Warfare Center (ONR-NSWC), 2002.

[44] Clockwise Solutions, "Notional Integrated Power System availability and total ownership cost," tech. rep., Clockwise Solutions Ltd., February 2002.

[45] Columbia Accident Investigation Board (CAIB), "CAIB final report," in *Vol. 1*, 2003.

[46] Comfort, L., *Shared risk: Complex systems in seismic response*. Pergamon, 1999.

[47] Conrow, E., *Effective Risk Management: Some Keys to Success*. American Institute of Aeronautics & Astronautics (AIAA), 2003.

[48] Costella, M., Saurin, T., and de Macedo Guimarães, L., "A method for assessing health and safety management systems from the resilience engineering perspective," *Safety Science*, vol. 47, no. 8, pp. 1056–1067, 2009.

[49] Cotsaftis, M., "What makes a system complex? an approach to self-organization and emergence." Online, June 2007.

[50] Council, H. S. A., "Report of the Critical Infrastructure Task Force," tech. rep., Department of Homeland Security, 2006.

[51] Couture, M., "Complexity and chaos - state-of-the-art; formulations and measures of complexity," Technical Note TN 2006-451, Defence R&D Canada - Valcartier, September 2007.

[52] Crawford, J., "Achieving resilient building designs for protection against structural collapse," tech. rep., Karagozian & Case, 2003.

[53] Creedy, S., "How miracle unfolded on qantas a380 at changi airport." online, December 2010.

[54] Dalziell, E. and McManus, S., "Resilience, vulnerability, and adaptive capacity: Implications for system performance," in *International Forum for Engineering Decision Making (IFED)*, Citeseer, 2004.

[55] Dandashi, F., "DoD architecture framework overview," October 2003.

[56] Darwin, C. and Carroll, J., *On the Origin of Species*. Broadview Press, 2003.

[57] Department of Defense (DoD), "System safety program requirements," 2000.

[58] Department of Defense (DoD), "Mandatory procedures for major defense acquisition programs (mdaps) and major automated information system (mais) acquisition programs." Online, 2002.

[59] Department of Defense (DoD), "Defenselink.com." Online, January 2009.

[60] Department of Defense, (DoD), "National security interests." online, 2010.

[61] Deutsch, M. and Willis, R., *Software Quality Engineering: A Total Technical and Management Approach*. Prentice-Hall, NJ, 1988.

[62] Dijkstra, A., "Resilience engineering and safety management systems in aviation," in *Second Symposium of the Resilience Engineering Network, L'Ecole de Mines de Paris, Sophia Antipolis, France*, 2007.

[63] Directive, E. C., "Oon the approximation of the laws of the member states relating to machinery." 89/392/EEC, 1989.

[64] Doerry, N., "Zonal ship design," *Naval engineers journal*, vol. 118, no. 1, pp. 39–53, 2006.

[65] Doerry, N., "Designing electrical power systems for survivability and quality of service," *Naval Engineers Journal*, vol. 119, no. 2, pp. 25–34, 2007.

[66] Doerry, N. and Davis, J., "Integrated Power System for marine applications," *NAVAL Engineers Journal*, vol. 106, pp. 77–90, 1994.

[67] Doerry, N., Robey, H., Amy, J., Petry, C., Adair, M., and Wyvill, R., "Powering the future with the Integrated Power System (IPS)," *Naval engineers journal*, vol. 108, no. 3, pp. 267–282, 1996.

[68] Drew, K., "The reconfigurable ship: Making it happen," in *ASNE Reconfiguration and Survivability Symposium*, February 2005.

[69] Dugdale, J. and Pavard, B., "Robustness and resilience in the design of emergency management systems," tech. rep., Laboratoire d'Informatique de Grenoble, France, 2009.

[70] Dunnington, L., Stevens, H., and Grater, G., "Integrated engineering plant for future naval combatants technology assessment and demonstration roadmap," Tech. Rep. MSD-50-TR-2003, Anteon Corporation, 2003.

[71] Ehlen, M., Vugrin, E., and Warren, D., "A resilience assessment framework for infrastructure and economic systems: Quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane.," tech. rep., Sandia National Laboratories, 2010.

[72] Ellison, R., Fisher, D., Linger, R., Lipson, H., Longstaff, T., and Mead, N., "Survivable network systems: An emerging discipline," tech. rep., Carnegie Mellon University, 1997.

[73] Ellison, R., Fisher, D., Linger, R., Lipson, H., Longstaff, T., and Mead, N., "An approach to survivable systems," in *NATO 1st Symposium on Protecting Information Systems in the 21st Century*, pp. 25–27, 1999.

[74] Ellison, R., Moore, A., Bass, L., Klein, M., and Bachmann, F., "Security and survivability reasoning frameworks and architectural design tactics," tech. rep., Carnegie Mellon University., 2004.

[75] Endsley, M., "Toward a theory of situation awareness in dynamic systems," *Ergonomics: Psychological mechanisms and models in ergonomics*, vol. 37, no. 1, p. 201, 2005.

[76] Environmental Protection Agency (EPA), "EPA Risk Assessment Process." online, April 2012.

[77] EPICC, *Earthquake Planning for Business*. Institute for Catastrophic loss Reduction, 2003.

[78] Ericson, A. and Ll, C., "Fault tree analysis," in *System Safety Conference, Orlando, Florida*, 1999.

[79] Fadier, E. and Ciccotelli, J., "How to integrate safety in design: Methods and models," *Human Factors and Ergonomics in Manufacturing & Service Industries*, vol. 9, no. 4, pp. 367–379, 1999.

[80] Fancher, P. and of Michigan, U., "Fostering development evaluation and deployment of Forward Crash Avoidance Systems (FOCAS)," tech. rep., NHTSA-UMTRI, 2000.

[81] Federal Aviation Administration (FAA), "Aircraft hardening program for aircraft safety and survivability." online, May 2009.

[82] Federal Aviation Administration (FAA), "Procedures for aircraft safety." Online, May 2009.

[83] Fiksel, J., "Designing resilient, sustainable systems," *Environ. Sci. Technol*, vol. 37, no. 23, pp. 5330–5339, 2003.

[84] Flack, G. and Kolevar, K. M., "Final report on the implementation of the task force recommendations," tech. rep., Natural Resources Canada and U.S. Department of Energy, 2006.

[85] Foote, R., "Mathematics and complex systems," *Science*, vol. 318, no. 5849, p. 410, 2007.

[86] Francis, P., "Defense acquisitions: Assessments of selected weapon programs," Tech. Rep. GAO-07-406SP, US Government Accountability Office (GAO), 2007.

[87] Ganesh, S., Schoder, K., Lai, H., Al-Hinai, A., and Feliachi, A., "Energy management system with automatic reconfiguration for electric shipboard power systems," in *Proc. of Reconfiguration and Survivability Symposium (RSS) 2005*, 2005.

[88] Gell-Mann, M., "What is complexity?," *Complexity*, vol. 1, no. 1, pp. 16–19, 1995.

[89] General Electric, "The Smart Grid." Online, January 2011.

[90] Globalsecurity.org, "USS Cole bombing." Online, 2004.

[91] Godschalk, D., "Urban hazard mitigation: Creating resilient cities," *Natural Hazards Review*, vol. 4, p. 136, 2003.

[92] Goode, H. and Machol, R., *System Engineering: An Introduction to the Design of Large-scale Systems*. McGraw-Hill, 1957.

[93] Graves, R., *The Greek Myths. Vol. 1*. Penguin, 1955. About Tiresias.

[94] Green, J. M. and Johnson, B. W., "Towards a theory of measures of effectiveness," tech. rep., Naval Postgraduate School, 2002.

[95] Grosan, C., Abraham, A., and Hassainen, A., "Designing resilient networks using multicriteria metaheuristics," *Telecommunication Systems*, vol. 40, no. 1, pp. 75–88, 2009.

[96] Grøtan, T., Størseth, F., Rø, M., and Skjerve, A., "Resilience, adaptation and improvisation–increasing resilience by organising for successful improvisation," in *3rd Symposium on Resilience Engineering, Antibes Juan-Les Pins, France October*, pp. 28–30, Citeseer, 2008.

[97] Habayeb, A., *System Effectiveness*. Pergamon, 1987.

[98] Haddad, W. and Corrado, J., "Robust resilient dynamic controllers for systems with parametric uncertainty and controller gain variations," *International Journal of Control*, vol. 73, no. 15, pp. 1405–1423, 2000.

[99] Haimes, Y., Crowther, K., and Horowitz, B., "Homeland security preparedness: Balancing protection with resilience in emergent systems," *Systems Engineering*, vol. 11, no. 4, pp. 287–308, 2008.

[100] Hammer, W., *Product Safety Management and Engineering*. Prentice-Hall, 1980.

[101] Hanifan, D. T., *Navy System Effectiveness Manual NAVMAT P3941-B*, Jul 1971-Sep 1973 1973.

[102] Harriss, R., Hohenemser, C., and Kates, R., *Energy Risk Management*, pp. 103–138. Academic Press, 1979.

[103] Hegner, H. and Desai, B., "Module level intelligent control system for integrated power systems," in *Thirteenth International Ship Control Systems Symposium (SCSS)*, (Orlando, Florida), April 2003.

[104] Heinrich, H., Petersen, D., and Roos, N., *Industrial Accident Prevention*. McGraw-Hill New York, 1950.

[105] Hockberger, W., "Total system ship design in a supersystem framework," *Total System Ship Design in a Supersystem Framework*, vol. null, p. null, 1996.

[106] Holling, C., "Resilience and stability of ecological systems," *Annual review of ecology and systematics*, vol. 4, no. 1, pp. 1–23, 1973.

[107] Holling, C., *Engineering Resilience Versus Ecological Resilience*, ch. Article 2, pp. 31–43. National Academy of Sciences, 1996.

[108] Hollnagel, E., "Accidents and barriers," in *Proceedings of lex valenciennes*, vol. 28, pp. 175–182, 1999.

[109] Hollnagel, E., "Resilience engineering: Why, what, and how," May 2007.

[110] Hollnagel, E. and Goteman, O., "The functional resonance accident model," in *Cognitive Systems Engineering in Process Control*, 2004.

[111] Hollnagel, E., Woods, D., and Leveson, N., *Resilience Engineering: Concepts and Precepts*. Ashgate Pub Co, 2006.

[112] Hootman, J. and Whitcomb, C., "A military effectiveness analysis and decision making framework for naval ship design and acquisition," *Naval Engineers Journal*, vol. 117, pp. 43–61, 2005.

[113] Horne, J. and Orr, J., "Assessing behaviors that create resilient organizations," *Employment Relations Today*, vol. 24, no. 4, pp. 29–39, 1997.

[114] Huber, S., van Wijgerden, I., de Witt, A., Dekker, S., and Hollnagel, E., "Resilience engineering: New directions for measuring and maintaining safety in complex systems," tech. rep., Lund University School of Aviation, 2007.

[115] Hughes, R., Balestrini, S., Kelly, K., Weston, N., and Mavris, D., "Modeling of an Integrated Reconfigurable Intelligent System (IRIS) for ship design," in *Ships & Ship Systems (S3) Technology Symposium Change, Challenges & Constants*, 2006.

[116] Hutchings, R., *American Diplomacy and the End of the Cold War: An Insider's Account of US Policy in Europe, 1989-1992*. Johns Hopkins Univ Pr, 1997.

[117] Hyslop, M., *Critical Information Infrastructures: Resilience and Protection*. Springer-Verlag New York Inc, 2007.

[118] International Maritime Organization (IMO), "Safety of Life at Sea, (SOLAS)," 1974.

[119] International Maritime Organization (IMO), "Safety Of Life At Sea (SOLAS) Amendments." online, May 2009.

[120] Janssen, M., Schoon, M., Ke, W., and Borner, K., "Scholarly networks on resilience, vulnerability and adaptation within the human dimensions of global environmental change," *Global Environmental Change*, vol. 16, no. 3, pp. 240–252, 2006.

[121] Jansson, J., Johansson, J., and Gustafsson, F., "Decision making for collision avoidance systems," *Intelligent vehicles: crash avoidance, safety, and driver information*, vol. 1662, p. 29, 2002.

[122] Jensen, H. J., *Self-Organized Criticality: Emergent Complex Behavior in Physical and Biological Systems*. Cambridge University Press, January 1998.

[123] Joint Chief of Staff, "Joint vision 2020." Online, 2003.

[124] Jones, B., Chandran, R., Cousens, E., Slotin, J., and Sherman, J., "From fragility to resilience: Concepts and dilemmas of statebuilding in fragile states," tech. rep., New York: New York University, Center on International Cooperation and International Peace Academy, Joint Program on Statebuilding as Peacebuilding, for OECD-DAC Fragile States Group, 2008.

[125] Kafali, C., "Application of fragility-based decision support methodologies," in *Student Research Accomplishments*, p. 23, School of Civil and Environmental Engineering, Cornell University, 2007.

[126] Kaplan, S., "The words of risk analysis," *Society for Risk Analysis*, vol. 17, pp. 407–417, June 1997.

[127] Kaplan, S. and Garrick, J., "On a quantitative definition of risk," *Journal Of Risk Analysis*, vol. 1, pp. 11–27, July 1980.

[128] Keel, L. and Bhattacharyya, S., "Robust, fragile, or optimal?," *Automatic Control, IEEE Transactions on*, vol. 42, no. 8, pp. 1098–1105, 1997.

[129] Keller, W. and Modarres, M., "A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: A tribute to the late professor norman carl rasmussen," *Reliability Engineering and System Safety*, vol. 89, pp. 271–285, August 2005.

[130] King, G., Schmill, M., Hannon, A., and Cohen, P., "Asymmetric Threat Assessment Tool (ATAT)," in *In Proceedings of the 14th Conference on Behavior Representation in Modeling and Simulation (BRIMS)* (Allender, L. and Kelley, T., eds.), (Orlando, FL), University of Arizona, May 2005.

[131] Kirby, M. and Mavris, D., "Forecasting the impact of technology infusion on subsonic transport affordability," in *1998 World Aviation Conference*, no. 985576, Georgia Institute of Technology, SAE International, September 1998.

[132] Knabb, R., Rhome, J., and Brown, D., "Tropical cyclone report: Hurricane Katrina: 23-30 august 2005," tech. rep., National Hurricane Center, 2005.

[133] Knight, J. and Sullivan, K., "Towards a definition of survivability," tech. rep., University of Virginia, 1997.

[134] Knight, J. and Sullivan, K., "On the definition of survivability," tech. rep., University of Virginia, 2000.

[135] Kuzma, H., Gorton, J., O'mara, J., Kelleher, P., and Rhoades, D., "Advanced damage control system concepts," in *Thirteenth International Ship Control Systems Symposium (SCSS)*, 2003.

[136] Laracy, J. and Leveson, N., "Applying STAMP to critical infrastructure protection," in *IEEE Conference on Technologies for Homeland Security*, (Boston, MA), 2007.

[137] Le Coze, J. and Dupré, M., "How to prevent a normal accident in a high reliable organisation: The art of resilience, a case study tn the chemical industry," in *Proceedings of the second resilience engineering symposium*, pp. 8–10, 2006.

[138] Lee, K. W., Higgins, J. J., and Tillman, F. A., "Stochastic models for mission effectiveness," *Reliability, IEEE Transactions on*, vol. 39, pp. 321–324, 328, Aug 1990.

[139] Lees, F., *Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control. Vols 1 and 2*. Butterworth-Heinemann, 1992.

[140] Leveson, N., *Safeware: System Safety and Computers*. ACM New York, NY, USA, 1995.

[141] Leveson, N., "White paper on approaches to safety engineering." White Paper on, 2003.

[142] Li, D., Li, J., and Zheng, Z., "Measuring nonequilibrium stability and resilience in an n-competitor system," *Nonlinear Analysis: Real World Applications*, vol. 11, no. 3, pp. 2016–2022, 2010.

[143] Littlefield, S. and Nickens, A., "Roadmap for the all-electric warship," *Power*, vol. 149, p. 46, February 2005.

[144] Lively, K. A., Scheidt, D. H., and Drew, K. F., "Mission based engineering plant control," tech. rep., Office of Naval Research, 2002.

[145] Lundberg, J., Johansson, B., and Johansson, L., "Resilience, stability and requisite interpretation in accident investigations," in *Proceedings of the Second Resilience Engineering Symposium*, pp. 191–198, Citeseer, 2006.

[146] Madni, A. and Jackson, S., "Towards a conceptual framework for resilience engineering," *Systems Journal, IEEE*, vol. 3, no. 2, pp. 181–191, 2009.

[147] Main, B., "Safety through design," September 2003.

[148] Mankins, J., "White paper on technology readiness levels." (White paper), 1995.

[149] Mansouri, M., Mostashari, A., and Nilchiani, R., "A decision analysis framework for resilience strategies in maritime systems," in *19th Annual INCOSE International Symposium (INCOSE 2009)*, 2009.

[150] Masud, A., Metcalf, P., and Hommertzheim, D., "A knowledge-based model management system for aircraft survivability analysis," *European Journal of Operational Research*, vol. 84, no. 1, pp. 47–59, 1995.

[151] Mavris, D., "The Ph.D process at ASDL," May 2007.

[152] Mavris, D. N. and DeLaurentis, D., "An integrated approach to military aircraft selection and concept evaluation," tech. rep., Aerospace System Design Laboratory, Georgia Institute of Technology, 1995.

[153] Mavris, D. N., DeLaurentis, D., Bandte, O., and Hale, M. A., "A stochastic approach to multi-disciplinary aircraft analysis and design," in *36th Aerospace Sciences Meeting & Exhibit, Reno, NV*, AIAA, January 1998.

[154] Mavris, D. and Bandte, O., "A probabilistic approach to multivariate constrained robust design simulation," in *AIAA and SAE, 1997 World Aviation Congress, Anaheim, CA*, 1997.

[155] McManus, H., Richards, M., Ross, A., and Hastings, D., "A framework for incorporating" ilities" in tradespace studies."," in *AIAA Space*, 2007.

[156] Merriam-Webster Dictionary, "Resilience." online, July 2011.

[157] Metz, S., *Armed Conflict in the 21st Century: The Information Revolution and Post-modern Warfare*. Strategic Studies Institute, 2000.

[158] Mikolášek, V., "Robustness in complex systems–state of the art report," Research Report 182-1/2008/26, Vienna University of Technology, 2008.

[159] Mileti, D., *Disasters by Design: A Reassessment of Natural Hazards in the United States*. Natl Academy Pr, 1999.

[160] Mitchell, S., Mannan, M., and O'Connor, M., "Designing resilient engineered systems," *Chemical Engineering Progress*, vol. 102, no. 4, pp. 39–45, 2006.

[161] Mitchell, S., *Resilient Engineered Systems: The Development of an Inherent System Property*. PhD thesis, Texas A&M University, 2007.

[162] Motulsky, H., *Intuitive biostatistics: a nonmathematical guide to statistical thinking*. Oxford Univ Pr, 2010.

[163] Mundy, C. E. and Kelso, F. B., *Naval Doctrine Publication 1 - Naval Warfare*. Department Of The Navy, Office Of The Chief Of Naval Operations, 1994.

[164] National Highway Traffic Safety Administration (NHTSA), "Annual collision statistics." online, May 2009.

[165] National Highway Traffic Safety Administration (NHTSA), "Consumer advisory: NHTSA's advice to Toyota customers." Online, February 10 2010.

[166] National Transportation Safety Board (NTSB), "Survivability of accidents involving part 121 U.S. Air Carrier Operations (1983-2000)," tech. rep., National Transportation Safety Board, 2001.

[167] Naval Safety Center, "Safety acquisition of naval systems." online, January 2011.

[168] Nelson, D., Adger, W., and Brown, K., "Adaptation to environmental change: Contributions of a resilience framework," *Annual review of Environment and Resources*, vol. 32, no. 1, p. 395, 2007.

[169] New York Independent System Operator (NYISO), "Interim report on the august 14, 2003 Blackout," tech. rep., New York Independent System Operator, January 2004.

[170] Newport, K., "Incorporating survivability considerations directly into the network design process," in *IEEE INFOCOM'90. Ninth Annual Joint Conference of the IEEE Computer and Communication Societies.'The Multiple Facets of Integration'. Proceedings.*, pp. 215–220, 1990.

[171] OPNAV Safety Liaison Office, "Executive overview: U.S. Navys acquisition safety website," June 2010.

[172] Panamair.org, "Pan Am Flight 103 bombing." Online, May 2009.

[173] Papanikolaou, A. and Boulougouris, E., "Design aspects of survivability of surface naval and merchant ships," tech. rep., National Technical University of Athens, 2003.

[174] Pate-Cornell, E., "Uncertainties in risk analysis: Six levels of treatment," *Reliability Engineering and System Safety*, vol. 54, pp. 95–111, 1996.

[175] Pekarek, S., Tichenor, J., Sudhoff, S., Sauer, J. D., Delisle, D., and Zivi, E., "Overview of a naval combat survivability program," tech. rep., University of Missouri, Purdue University, Naval Surface Warfare Command, U.S. Naval Academy, 2002.

[176] Perrow, C., *Normal Accidents*. Princeton University Press, 1984.

[177] Phadke, M., *Quality Engineering Using Robust Design*. Prentice Hall PTR Upper Saddle River, NJ, 1995.

[178] Pimm, S., *The Balance of Nature?: Ecological Issues in the Conservation of Species and Communities*. University of Chicago Press, 1991.

[179] Popovici, E., Bucci, A., and Gaudiano, P., "Evolutionary design of control algorithms for hydraulic systems," October 2008.

[180] Poroseva, S., Woodruff, S., and Hussaini, M., "Designing survivable power systems," in *IEEE/PES Transmission and Distribution Conference and Exposition, 2008. T&D*, pp. 1–7, 2008.

[181] President Obama, B., "National Preparedness Month 2009." online, September 2009.

[182] Rains, D., "Combatant ship design guidance through mission effectiveness analysis," *Naval Engineers Journal*, vol. 96, no. 3, pp. 112–127, 1984.

[183] Rasmussen, J., "Risk management in a dynamic society: A modelling problem," *Safety Science*, vol. 27, no. 2/3, pp. 183–213, 1997.

[184] Rausand, M., "Reliability centered maintenance," *Reliability Engineering and System Safety*, vol. 60, pp. 121–132, 1998.

[185] Rausand, M. and Oien, K., "The basic concepts of failure analysis," *Reliability Engineering and System Safety*, vol. 53, pp. 73–83, 1996.

[186] Reason, J., *Human Error*. Cambridge University Press, 1990.

[187] Reason, J., "Managing the risks of organizational accidents," October 2004.

[188] Reed, D., Kapur, K., and Christie, R., "Methodology for assessing the resilience of networked infrastructure," *Systems Journal, IEEE*, vol. 3, no. 2, pp. 174–180, 2009.

[189] Reich, J., Zautra, A., and Hall, J., *Handbook of Adult Resilience*. The Guilford Press, 2010.

[190] Richards, M., *Multi-Attribute Tradespace Exploration for Survivability*. PhD thesis, Engineering Systems Division, Massachusetts Institute of Technology,, Cambridge, MA, 2009.

[191] Richards, M. G., Hastings, D. E., Rhodes, D. H., and Weigel, A. L., "Defining survivability for engineering systems," tech. rep., Engineering Systems Division, Massachusetts Institute of Technology,, 2008.

[192] Richards, M. G., Hastings, D. E., Rhodes, D. H., and Weigel, A. L., "Systems architecting for survivability: Limitations of existing methods for aerospace systems," tech. rep., Engineering Systems Division, Massachusetts Institute of Technology,, 2008.

[193] Richards, M. G., Ross, A. M., Hastings, D. E., and Rhodes, D. H., "Design principles for survivable system architectures." White paper, 2006.

[194] Rieger, C., Gertman, D., and McQueen, M., "Resilient control systems: Next generation design research," in *Human System Interactions, 2009. HSI'09. 2nd Conference on*, pp. 632–636, IEEE, 2009.

[195] Roland, H. and Moriarty, B., *System Safety Engineering and Management*. Wiley-Interscience, 1990.

[196] Rose, A., "Economic resilience to natural and man-made disasters: Multidisciplinary origins and contextual dimensions," *Environmental Hazards*, vol. 7, no. 4, pp. 383–398, 2007.

[197] Rose, A. and Liao, S., "Modeling regional economic resilience to disasters: A computable general equilibrium analysis of water service disruptions*," *Journal of Regional Science*, vol. 45, no. 1, pp. 75–112, 2005.

[198] Ross, A., *Managing unarticulated value: changeability in multi-attribute tradespace exploration*. PhD thesis, Engineering Systems Division, Massachusetts Institute of Technology,, 2006.

[199] Rostker, B., "Navy actions needed to optimize ship crew size and reduce total ownership costs. GAO Report To Congress 2003," Tech. Rep. GAO-03-520, US Government Accountability Office, 2003.

[200] Rudwick, B., *Systems Analysis for Effective Planning: Principles and Cases*. John Wiley & Sons, 1969.

[201] Rumsfeld, D., "The national defense strategy of the united states of america," 2005.

[202] Ryan, M. E., "Air force and space basic doctrine." Online, September 1997.

[203] S-18, A., "Certification considerations for highly-integrated or complex aircraft systems," 11 1996.

[204] SAFER EURORO, "Design for safety: An integrated approach to safe european Ro-Ro ferry design," tech. rep., EU Industrial and Materials Technologies (BRITE-EURAM III) Programme, 2003.

[205] Sage, A. and Armstrong, J., *Introduction to Systems Engineering*. Wiley New York, 2000.

[206] Said, M., "Theory and practice of total ship survivability for ship design," *Naval Engineers Journal*, vol. 107, no. 4, pp. 191–203, 1995.

[207] Scheidt, D. H., "Intelligent agent-based control," *Johns Hopkins APL Technical Digest*, vol. 23, no. 4, pp. 383–395, 2002.

[208] Schleher, D., "Introduction to electronic warfare," tech. rep., Eaton Corp., AIL Div., Deer Park, NY, 1986.

[209] Schwartz, C. R., "JTCG/AS aerospace systems survivability handbook series - volume 1. series overview," tech. rep., Joint Technical Coordinating Group on Aircraft Survivability (JTCG/AS), 2001.

[210] Schwartz, G., "Reliability and survivability in the reduced ships crew by virtual presence system," tech. rep., Charles Stark Draper Laboratory Inc., 2001.

[211] Seville, E., "Resilience: Great concept but what does it mean?." online, 2008.

[212] Shinozuka, M., Chang, S. E., Cheng, T.-C., Feng, M., ORourke, T. D., Saadeghvaziri, M. A., Dong, X., Jin, X., Wang, Y., and Shi, P., "Resilience of integrated power and water systems," in *Seismic Evaluation and Retrofit of Lifeline Systems*, Multidisciplinary Center for Earthquake Engineering Research (MCEER), 2008.

[213] Shlapak, D., *A Global Access Strategy for the US Air Force*. Rand Corp, 2002.

[214] Sklet, S., "Methods for accident investigation," Report ROSS (NTNU) 200208, NTNU Norwegian University of Science and Technology, N-7491 Trondheim, November 2002.

[215] Sklet, S., "Comparison of some selected methods for accident investigation," *Journal of Hazardous Materials*, vol. 111, pp. 29–37, April 2004.

[216] Sklet, S., "Safety barriers: Definition, classification, and performance," *Journal of Loss Prevention in the Process Industries*, vol. 19, pp. 494–506, December 2006.

[217] Soban, D., *A Methodology for the Probabilistic Assessment of System Effectiveness as Applied to Aircraft Survivability and Susceptibility.* PhD thesis, Georgia Institute of Technology, November 2001.

[218] Soban, D. and Mavris, D., "The need for a military system effectiveness framework - the system of systems approach," in *AIAA, Aircraft, Technology Integration, and Operations Forum, 1 st, Los Angeles, CA*, 2001.

[219] Soni, S., Gupta, R., and Pirkul, H., "Survivable network design: The State Of The Art," *Information Systems Frontiers*, vol. 1, no. 3, pp. 303–315, 1999.

[220] Stamatelatos, M., Apostolakis, G., Dezfuli, H., Everline, C., Guarro, S., Moieni, P., Mosleh, A., Paulos, T., and Youngblood, R., *Probabilistic Risk Assessment Procedures Guide for Nasa Managers and Practitioners.* NASA Office of Safety and Mission Assurance, v1.1 ed., 2002.

[221] Stamatis, D., *Failure mode and effect analysis: FMEA from theory to execution.* Asq Pr, 2003.

[222] Stoessinger, J., *Why Nations Go to War.* St. Martin's Press, 1993.

[223] Stringfellow, M., "Safety-driven system engineering process," Master's thesis, Massachusetts Institute of Technology. Dept. of Aeronautics and Astronautics., 2008.

[224] Sturtevant, G., Socoloski, P., Bartlett, D., and Totimeh, L., "US Navy Smart Ship integrated ship controls: Technology roadmap for performance enhancements," in *13th International Ship Control Systems Symposium in Orlando, FL*, pp. 7–9, 2003.

[225] Sudhoff, S., Zivi, E., and McCoy, T., "Thoughts on survivability performance metrics and an approach to integrated engineering plant modeling." White Paper, 2004.

[226] Sudhoff, S., Pekarek, S., Kuhn, B., Glover, S., Sauer, J., and Delisle, D., "Naval combat survivability testbeds for investigation of issues in shipboard power electronics based power and propulsion systems," in *IEEE Power Engineering Society Summer Meeting*, vol. 1, 2002.

[227] Suh, N., *The Principles of Design.* Oxford University Press, USA, 1990.

[228] SURVICE Engineering Company, "Survivability and UAVs," January 2002.

[229] Syntek Technologies, "DD(X) notional baseline modeling and simulation development report," tech. rep., Florida State University, Center for Advanced Power Systems, August 2003.

[230] Taguchi, G. and Organization, A. P., *Introduction to quality engineering: designing quality into products and processes*. The Organization Tokyo, 1986.

[231] Tarvainen, P., "Survey of the survivability of IT systems," in *Proceedings of the Ninth Nordic Workshop on Secure IT Systems. Helsinki, University of Technology*, pp. 15–20, 2004.

[232] The Committe on Armed Services, "The attack on the U.S.S. Cole," tech. rep., U.S. House of Representatives, Washington, October 2000.

[233] The Institute for Telecommunication Sciences, "1037c: Glossary of telecommunications terms." online, October 2006.

[234] Tierney, K. and Bruneau, M., "Conceptualizing and measuring resilience: a key to disaster loss reduction," in *TR News*, no. 250 in TR News, Transportation Research Board (TRB), 2007.

[235] Tinker, P., Azuma, R., Hein, C., and Daily, M., "Driving simulation for crash avoidance warning evaluation," in *Proceedings of 29 th ISATA Dedicated Conference on Simulation, Diagnosis and Virtual Reality in the Automotive Industry*, pp. 367–374, 1996.

[236] Tyrell, D., Severson, K., and Marquis, B., "Train crashworthiness design for occupant survivability," *Power*, vol. 25, p. 4, 1995.

[237] U.S. Air Force, "The US Air Force Transformation Flight Plan." online, 2003.

[238] U.S. Army, *Field Manual (FM) 3-0, Operations*, 2001.

[239] U.S. Coast Guard, "Coast Guard Publication 1," *Washington, DC: January*, vol. 1, 2002.

[240] U.S. Code, "Title 10 - Armed Forces." online, 1986.

[241] US Federal Emergency Management Agency (FEMA), "System resilience definition," 2002.

[242] U.S. Government, "National defense strategy 2005," 2005.

[243] U.S. Marine Corps., "Marine Corps Doctrinal Publication (MCDP) 1-0,." online, 2001.

[244] U.S. Marine Corps., *Warfighting*. Cosimo Inc, 2007.

[245] U.S. Navy, *U.S. Navy Survavibility Design Handbook For Surface Ships*. Chief of Naval Operations Ship Safety and Survivability Office, OPNAV P-86-4-99 ed., September 2000.

[246] U.S. Navy, "Mission need statement for a 21st century surface combatant," tech. rep., U.S. Navy, 2002.

[247] U.S. Navy, "Mission of the navy." online, June 2011.

[248] Venkatasubramanian, V., Malik, T., Raghavendra, P., Shukla, A.and Villez, K., Rieger, C., Daum, K., and McQueen, M., "RNEDE: Resilient Network Design Environment," August 2010.

[249] Vidal, M., Carvalho, P., Santos, M., and Santos, I., "Collective work and resilience of complex systems," *Journal of Loss Prevention in the Process Industries*, vol. 22, no. 4, pp. 516–527, 2009.

[250] Villez, K., Venkatasubramanian, V., and Rieger, C., "Resilient design of recharging station networks for electric transportation vehicles," August 2011.

[251] Vugrin, E., Warren, D., Ehlen, M., and Camphouse, R., "A framework for assessing the resilience of infrastructure and economic systems," in *Sustainable and Resilient Critical Infrastructure Systems: Simulation, Modeling, and Intelligent Engineering*, p. 77, Springer Verlag, 2010.

[252] Walker, B., Gunderson, L., Kinzig, A., Folke, C., Carpenter, S., and Schultz, L., "A handful of heuristics and some propositions for understanding resilience in social-ecological systems," *Ecology and Society*, vol. 11, no. 1, p. 13, 2006.

[253] Walks, J. and Grater, G., "Integrated Engineering Plant: Whats it really all about," August 2004.

[254] Wallace, J., *A Framework for Conducting Mechanistic Based Reliability Assessments of Components Operating in Complex Systems*. PhD thesis, School of Aerospace Engineering, Georgia Institute of Technology, 2003.

[255] Wallensteen, P., *Understanding Conflict Resolution: War, Peace and the Global System*. Sage, 2002.

[256] Wang, D. and Ip, W., "Evaluation and analysis of logistic network resilience with application to aircraft servicing," *Systems Journal, IEEE*, vol. 3, no. 2, pp. 166–173, 2009.

[257] Wei, D. and Kun Ji, K., "Resilient Industrial Control System (RICS): Concepts, formulation, metrics, and insights," August 2010.

[258] Weick, K. and Sutcliffe, K., *Managing the unexpected: Assuring high performance in an age of complexity*. San Francisco, CA: Jossey-Bass, 2001.

[259] Weldon, W., Gale, P., Adair, R., Adamiak, M., Allen, C., Ashton, R., Brown, C., Felton, L., Fischl, R., Gully, J., Hubbard, J., Kohn, E., Mulholland, M., Neal, W., Norton, P., Smith, K., Stamp, J., Stevens, H., Tozzi, J., Winter, T., and Young, S., "Roadmap to an Electric Naval Force," group study, Naval Research Advisory Committee, 2002.

[260] Westrum, R., "All coherence gone: New orleans as a resilience failure," in *Second Symposium on Resilience Engineering Proceedings*, (Juan-les-Pins, France), pp. 8–10, November 2006.

[261] Wilbur, A., "Metrics guidebook for integrated systems and product development, international council on systems engineering," tech. rep., INCOSE-TP-1995-002-01, 1995.

[262] Wildavsky, A., *Searching for safety*. Transaction Books, 1988.

[263] Williams, F., "DC-ARM final demonstration report," tech. rep., Naval Research Laboratory (NRL), 2003.

[264] Willinger, W. and Doyle, J., "Robustness and the internet: Design and evolution," in *Informational (p.21) 3426 Architectural and Policy Considerations*, 2002.

[265] Woods, D., "Creating foresight: How resilience engineering can transform NASA's approach to risky decision making," *Work*, vol. 4, no. 2, pp. 137–144, 2003.

[266] Yarbrough, N. and Kupferer, R., "The Joint Command and Control Ship (JCC (X)) approach to survivability requirements development: Total ship survivability assessment," in *Association of Scientists and Engineers–38th Annual Technical Symposium*, 2002.

[267] Youn, B., Choi, K., Yang, R., and Gu, L., "Reliability-based design optimization for crashworthiness of vehicle side impact," *Structural and Multidisciplinary Optimization*, vol. 26, no. 3, pp. 272–283, 2004.

[268] Zivi, E. and McCoy, T., "ONR ship control challenge problem," in *Thirteenth International Ship Control Systems Symposium (SCSS)*, 2003.

VITA

Michael Gregory Balchanos was born March 31, 1980 and is a native of Thessaloniki, Greece. After spending most of his childhood in Alexandria Imathias, in 1992 he returned to Thessaloniki for his high school education. He attended the Experimental School of Aristotle University of Thessaloniki, from which he graduated in 1997. During the same year, he was admitted in the Department of Physics, School of Natural Sciences of the Aristotle University of Thessaloniki. As an undergraduate student, Mr. Balchanos completed a minor in Electronics and Telecommunications during his senior year. After completing his Degree Thesis, titled as "Chaos in fluid dynamical systems", he obtained his Diploma in Physics from the Aristotle University of Thessaloniki in 2002. Motivated by his exposure to applied engineering problems in fluid dynamics, he decided to continue his graduate studies in the field of Aerospace engineering. Upon his admittance by the Georgia Institute of Technology, he joined the Aerospace Systems Design Laboratory (ASDL) in 2004. Under the supervision of Dr. Dimitri Mavris, he obtained his M.S. degree in Aerospace Engineering in 2005, and he completed all requirements for his Ph.D degree in 2012.

During his ASDL tenure, Mr. Balchanos has been working on the Integrated Reconfigurable Intelligent Systems (IRIS) Initiative, funded by the Office of Naval Research (ONR). His research interests have been evolving in parallel to the needs and lessons learned from his IRIS research experience. Some of his early research directions include electric power generation and distribution systems modeling and simulation, damage propagation modeling in complex systems, as well as computational integration methods for dynamic naval system models. As part of his support to IRIS, he has been expanding his research portfolio to include naval architecting,

computer-aided naval ship design. He had also been involved into application problems similar to IRIS, such as the GE-funded Smart Grid Initiative, and other ONR sponsored programs. As part of his thesis topic exploration, he has been investigating analysis methods for complex dynamical system resilience and survivability assessment under changing environmental conditions. His methods have been applied on naval system architectures. In his very limited free time, he enjoys working out, listening to good music and following the automotive industry and formula 1.